Дата поступления рукописи в редакцию: 12.08.2026 г.
Дата принятия рукописи в печать: 25.09.2026 г.

DOI: 10.24412/2782-3849-2026-9-308-323

ТАРАСОВ Александр Анатольевич,
старший преподаватель Департамента уголовного права, процесса и криминалистики Факультета права Национального исследовательского университета «Высшая школа экономики» (НИУ ВШЭ), ORCID:0000-0078-9276-5211, ResearcherID: T-8912-2023, Scopus AuthorID: 82640173651, e-mail: tarasov.aa@hse.ru

ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ OSINT В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ И КОРПОРАТИВНОЙ БЕЗОПАСНОСТИ

Аннотация. *В статье приведены результаты исследования теоретико-практических аспектов правового регулирования применения OSINT-технологий (мониторинг на основе открытых источников). Проанализирована его двойственная сущность как инструмента государственно-властной деятельности в рамках ОРД и механизма обеспечения корпоративной безопасности. Обосновано, что методы анализа открытых данных прочно закрепились в практике корпоративного контроля и используются в качестве базового инструмента в контуре корпоративного антикоррупционного комплаенса, процедуре комплексной проверки контрагентов и установления реальных выгодоприобретателей.*

Выявлены системные ключевые правовые риски, связанные с возможным нарушением конституционных прав граждан на неприкосновенность частной жизни, личную тайну (ст. 23, 24 Конституции РФ), и квалификацией действий сотрудников служб безопасности по ст. 137, 138 и 272 УК РФ.

Особое внимание в исследовании уделено концепции динамического статуса данных в Интернете, предопределяющей способность одного и того же массива цифровой информации изменять свой правовой режим под влиянием внешних условий, действий пользователя или алгоритмов платформ, а также правовой оценке неправомерного использования утекших баз данных в теневом сегменте веб-пространства Даркнет.

По итогам исследования предлагается комплекс законодательных изменений, в том числе дополнение ФЗ «Об ОРД» новым оперативно-розыскным мероприятием и разработка стандартов цифровой проверки для коммерческого сектора.

Ключевые слова: *OSINT, открытые источники, оперативно-розыскная деятельность, корпоративная безопасность, персональные данные, защита приватности, уголовная ответственность, цифровые следы, базы утечек.*

TARASOV Aleksandr Anatolyevich,
Senior Lecturer at the Department of Criminal Law, Procedure and Criminology, Faculty of Law, National Research University Higher School of Economics (HSE University)

PROBLEMS OF LEGAL REGULATION OF OSINT IN OPERATIONAL-INVESTIGATIVE ACTIVITIES AND CORPORATE SECURITY

Annotation. *The article presents the results of a study on the theoretical and practical aspects of the legal regulation of open-source intelligence (OSINT) technologies. The dual nature of OSINT is analyzed as both a tool of state-authoritative activity within the framework of operational-investigative activities and a mechanism for ensuring corporate security. It is substantiated that open data analysis methods have become firmly established in the practice of corporate control and are used as a core tool within corporate anti-corruption compliance, counterparty due diligence procedures, and the identification of ultimate beneficial owners.*

Systemic key legal risks are identified, including potential violations of citizens' constitutional rights to privacy and personal secrecy (Articles 23 and 24 of the Constitution of the Russian Federation), as well as the criminal qualification of security services' actions under Articles 137, 138, and 272 of the Criminal Code of the Russian Federation.

Special attention is paid to the concept of the dynamic status of Internet data, which determines the ability of a digital information array to alter its legal regime under the influence of external

conditions, user actions, or platform algorithms, alongside a legal assessment of the illicit use of leaked databases in the dark web (Darknet).

Based on the research findings, a comprehensive set of legislative amendments is proposed, including supplementing the Federal Law "On Operational-Investigative Activities" with a new operational-investigative measure and developing digital verification standards for the commercial sector.

Key words: *OSINT, open sources, operational-investigative activity, corporate security, personal data, privacy protection, criminal liability, digital footprints, leaked databases.*

1. Введение

Согласно консолидированным статистическим отчетам ведущих международных аналитических агентств, к началу 2026 году совокупный объем глобальной информационной сферы превысил 175 зеттабайт. Если записать указанный объем на стандартные Blu-ray диски (по 25 ГБ) и сложить их в стопку, она дойдет до Луны и обратно 23 раза и составит около 17 682 400 километров. При этом более 80% из них составляют неструктурированные пользовательские цифровые следы, логи, медиафайлы и метаданные, находящиеся в условно открытом доступе [1].

Цифровая трансформация общественных отношений и взрывной рост объема информации, ежедневно появляющейся в мировой сети, существенно поменяли деятельность государства по защите своих интересов, а также подходы частного сектора экономики по выстраиванию корпоративной безопасности. В условиях повсеместного использования больших данных и систем искусственного интеллекта, мониторинг по открытым источникам (OSINT) становится одним из ключевых инструментов информационно-аналитической работы.

В подтверждение данного тезиса профессор В. Б. Исаков отмечает: «Информатизация, интеллектуализация государственного управления и бизнеса является одной из основных тенденций последних десятилетий. Происходящие изменения видны "невооруженным глазом": расширяется область применения компьютеров, средств передачи данных, информационных технологий; увеличивается круг информационно-аналитических задач в управлении; растет число "интеллектуальных фирм", предлагающих свои услуги государственному управлению и бизнесу» [2].

Речь идет об автоматизированном сборе данных, их парсинге (Парсинг (веб-скрейпинг) — это процесс автоматического сбора данных с веб-сайтов, веб-страниц или из файлов. Специальная программа (парсер) заходит на сайт, находит нужную информацию и сохраняет её в структурированном виде), предиктивном анализе и сведении воедино цифровых следов, включая метаданные, публикации в социальных медиа и данные из государственных реестров. Все это уже активно используют и правоохранительные органы, и корпоративные службы безопасности

Классическое "аналоговое" законодательство больше не успевает за скоростью технологического прогресса. Динамичное развитие цифрового базиса OSINT вошло в острое противоречие с консервативной правовой надстройкой. В настоящее время в Российской Федерации полностью отсутствует профильное нормативное регулирование "цифровой разведки", что порождает критические правовые риски.

Так, при проведении оперативно-розыскной деятельности размытость дефиниции "открытых данных", что создает угрозу несанкционированного проникновения в частную жизнь граждан, нарушая конституционные гарантии неприкосновенности личной тайны (ст. 23, 24 Конституции РФ).

В секторе корпоративной безопасности применение инструментов OSINT балансирует на грани уголовно-наказуемых деяний, связанных с незаконным оборотом персональных данных (ст. 137 УК РФ), а также неправомерным доступом к компьютерной информации (ст. 272 УК РФ). Ситуация усугубляется практикой использования корпоративными аналитиками массивов информации, хранящейся в условиях облачных технологий, а также утекших в теневой сегмент сети Интернет (Даркнет). Несмотря на то, что такие базы де-факто находятся в публичном доступе, их обработка де-юре также образует состав правонарушения.

На этом фоне существующий научно-теоретический и практический дискурс демонстрирует, что правовая доктрина не предлагает четких критериев разграничения легального сбора общедоступной информации и противоправного вмешательства в сферу конфиденциальных данных. Цифровая трансформация создала тройственный конфликт интересов, где оперативно-розыскная деятельность государства и организуемые бизнесом меры по защите своих активов, а также комплаенс-проверка контрагентов неизбежно ущемляют базовые права граждан на цифровую приватность.

Заявленная проблематика носит выраженный междисциплинарный характер и находится на стыке двух крупных научных направлений. В частности, государственно-правовой аспект исследования охватывает анализ административных информационных режимов, опреде-

ление конституционных границ государственного вмешательства в частную жизнь граждан, а также правовое позиционирование цифровых платформ. В преломлении уголовно-правового научного направления фокус смещается на оценку результатов OSINT-мероприятий как ориентирующей информации или средств доказывания (в контексте ст. 89 УПК РФ), верификацию цифровых улик (риски дипфейк-технологий и фальсификации логов) и материально-правовую квалификацию преступлений, совершаемых с использованием ИИ и интернет-технологий.

В современный период ключевой вклад в развитие доктрины цифрового права, правового статуса искусственного интеллекта и сквозных технологий вносят исследования ведущих отечественных правоведов, чьи труды можно разделить на несколько ключевых направлений. Во-первых, это формирование общей теории и методологии цифровизации публичной власти, права и законодательного процесса (Т. Я. Хабриева [3], Ю. А. Тихомиров [4]), а также обоснование концепции цифрового права как комплексного института на базе масштабных междисциплинарных исследований (В. В. Блажеев, М. А. Егорова [5]). Во-вторых, это разработка фундаментальных основ правового регулирования цифровой экономики, интернет-права, а также этических и правовых аспектов применения искусственного интеллекта (В. А. Вайпан [6], В. В. Архипов [7]).

В-третьих, это глубокий анализ правовых режимов искусственного интеллекта, медиапространства, технологии "дипфейк", методологии информационного права и информационной безопасности (В. А. Виноградов, Д. В. Кузнецова [8], И. Ю. Богдановская [9], А. В. Минбалеев [10], П. У. Кузнецов [11], И. А. Филипова [12]). В-четвертых, это исследования в сфере регулирования цифровых прав, интеллектуальной собственности (IP-права) и правового статуса виртуального имущества (Л. А. Новоселова, М. А. Рожкова). Наконец, применительно к уголовно-правовым, процессуальным и криминалистическим аспектам обеспечения цифровой безопасности государства и бизнеса особое значение имеют труды Л. А. Воскобитовой [13], а также С. В. Расторопова и В. А. Прорвича [14].

Объект исследования составляют общественные отношения, складывающиеся субъектами оперативно-розыскной деятельности и институтами корпоративной безопасности в процессе применения технологий мониторинга открытых источников (OSINT).

Предмет исследования охватывает нормы конституционного, уголовного, оперативно-розыскного и информационного законодательства РФ, регулирующих оборот цифровых данных, а также соответствующую судебно-следственную практику.

Цель исследования состоит в разработке основы для комплексной, научно обоснованной концепции правового регулирования OSINT в РФ, позволяющей удержать баланс между интересами государственной безопасности, защитой бизнеса и соблюдением конституционных прав граждан. Реализация цели исследования предполагает решение задач по нормативному определению понятийного аппарата OSINT, разрешению коллизий его применения в ОРД и корпоративном секторе (с оценкой уголовно-правовых рисков), а также формированию законодательных предложений по легализации результатов интернет-мониторинга.

Методологическую основу исследования составили общенаучные методы (анализ, синтез, системно-структурный подход) и специальные юридические методы: формально-догматический (при анализе ст. 137, 138, 272 УК РФ), сравнительно-правовой (анализ подходов к приватности в РФ и зарубежных доктрин, опирающихся на принцип обоснованных ожиданий неприкосновенности частной жизни) и метод правового моделирования.

2. Понятие, сущность OSINT в современном правовом поле

В современной доктрине информационного, уголовного и публичного права феномен OSINT (Open Source Intelligence) традиционно рассматривается сквозь призму междисциплинарного подхода. Зародившись в недрах специальных служб как методология ведения оборонной разведки, в условиях тотальной цифровизации общества OSINT трансформировался в универсальный правовой и технологический инструмент.

Нельзя не согласиться с позицией исследователей М. О. Янгаевой и Н. О. Павленко о том, что «с помощью OSINT можно не только проводить сбор данных в социальных сетях, но также использовать расширенные запросы поисковых систем для предоставления наиболее точных результатов поиска, осуществлять поиск удаленных версий веб-сайтов, отслеживать людей и их деятельность в Интернете с помощью общедоступных баз данных и эффективных инструментов поиска, просматривать спутниковые изображения любой улицы мира, искать геолокацию лица и многое другое» [15].

В этой связи в контексте юриспруденции OSINT можно определить как основанную на нормах действующего законодательства комплексную систему организационных, технических и аналитических мер по поиску, сбору, систематизации и оценке юридически значимой информации, полученной из легально доступных источников, с целью информационного обеспечения

публично-правовой деятельности (включая ОРД) либо защиты частноправовых интересов (корпоративной безопасности).

М. О. Янгаевой и Н. О. Павленко отмечают, что «в своих целях OSINT используют: государственные структуры (для обеспечения национальной безопасности, борьбы с разными видами терроризма и т.д.); международные организации; бизнес-корпорации (для исследования новых рынков, мониторинга деятельности конкурентов, планирования маркетинговой деятельности и т.д.); преступные организации (для сбора данных о конкретной цели в сети Интернет)» [15].

Ключевая научно-теоретическая и правоприменительная проблема заключается в юридической квалификации информационных массивов, вовлекаемых в орбиту OSINT. Российское и международное законодательство проводят жесткую границу между институтом «открытых данных» (Open Data) и массивами информации, "доступ к которым формально ограничен нормативными актами, но технически остается возможным".

Так, открытыми данными (Open Data) принято считать информацию, размещенную ее правообладателями (включая государственные органы) в сети Интернет в формате, допускающем ее автоматизированную обработку без введения каких-либо технических или юридических цензов на ее повторное использование (ст. 7 Федерального закона № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [16]).

Примерами служат открытые реестры ФНС, ЕГРЮЛ, порталы госзакупок, данные которых априори не обладают признаком конфиденциальности.

К категории информации, доступ к которой ограничен, но технически возможен относятся сведения, защищенные законодательством о персональных данных, коммерческой, банковской, врачебной и иной тайне, доступ к которым заблокирован владельцем (например, приватные аккаунты в социальных сетях, архивированные логи, удаленные из кэша веб-страницы, а также массивы данных, утекшие в результате деликтов в Darknet).

С технической точки зрения аналитик OSINT имеет возможность обойти установленные ограничения, используя уязвимости API платформ, методы социальной инженерии, деанонимизацию через связанные узлы или обращение к серверам утечек. С публично-правовой позиции преодоление таких барьеров без надлежащих законных оснований (судебного решения или прямого полномочия) переводит деятельность из легального поля OSINT в сферу правонарушений, предусмотренных ст. 137, 272 УК РФ или законодательством о персональных данных [16].

Современный инструментарий OSINT базируется на алгоритмах высокоскоростной обработки неструктурированной информации, что коренным образом меняет процессуальный и материальный статус собираемых сведений. К основным сквозным технологиям, используемым субъектами ОРД и корпоративной безопасности, относятся: парсинг и скрапинг (автоматизированный сбор данных). Использование скриптов и программного обеспечения (например, библиотек на языке Python) для мгновенного извлечения информации с тысяч веб-страниц. При этом основной правовой риск заключается в нарушении пользовательских соглашений платформ и преодолении технических барьеров защиты.

В правовом контексте остается дискуссионным вопрос квалификации обхода технических запретов сайта в качестве «неправомерного доступа» по смыслу статьи 272 УК РФ [17], если сама информация изначально размещена пользователем в публичном профиле. Сложность данной квалификации усугубляется спецификой применяемых при этом технологических методов сбора данных, которые выходят за рамки обычного ознакомления с контентом.

Так, правовые риски интеграции OSINT-технологий во многом связаны со сбором и анализом метаданных (геолокации, временных меток, технических характеристик устройств и идентификаторов авторов). Извлечение этих скрытых параметров из графических или текстовых документов служит эффективным инструментом верификации цифровых следов. Однако аккумулирование подобных сведений без согласия субъекта нарушает установленные ФЗ № 152-ФЗ [18] принципы соразмерности и целевой направленности обработки персональных данных.

Аналогичные коллизии возникают при внедрении нейросетевых моделей и алгоритмов искусственного интеллекта (включая распознавание лиц, предиктивную аналитику, графический и семантический анализ текстов). Инструментарий ИИ позволяет интегрировать разрозненные цифровые следы в комплексный профиль личности. Правовая специфика данной ситуации заключается в том, что агрегированная из открытых источников информация на выходе приобретает признаки специальных категорий персональных данных (раскрывающих политические взгляды, религиозные убеждения или маршруты перемещения граждан), что де-факто требует применения режима повышенной правовой защиты, установленного ст. 10 ФЗ «О персональных данных» [18].

Зарубежная правовая мысль сформировала более гибкие доктринальные подходы к разграничению легитимного использования методов OSINT и противоправного скрытого наблюдения,

представляющие фундаментальный интерес для отечественной науки.

Данное регулирование в США осуществляется как на федеральном уровне, так и на уровне штатов. Это объясняется устройством государства, которое сложилось исторически [19]. «В американской модели федерализма 50 штатов, образующих Соединенные Штаты Америки, располагают большим объемом независимости и власти. По сути дела США — это страна, состоящая из 51 различного государства: 50 государственных механизмов штатов и отдельного федерального государственного механизма. В каждом из этих механизмов имеется своя правовая система» [20].

В США ключевым регулятором применения OSINT государственными органами выступают положения Четвертой поправки к Конституции, защищающей граждан от необоснованных обысков и изъятий. Граница правомерности OSINT в американской юриспруденции определяется прецедентной концепцией правомерных ожиданий конфиденциальности (обоснованных ожиданий неприкосновенности частной жизни), сформулированной Верховным судом США в Деле «Кац против Соединенных Штатов» (1967) [21].

Согласно данной доктрине, правовая защита активируется если субъект объективно продемонстрировал намерение сохранить информацию в тайне и одновременно общество признает данное ожидание разумным и обоснованным. В контексте OSINT сведения, сознательно размещенные пользователем в открытом профиле социальной сети, не подпадают под действие Четвертой поправки, что освобождает правоохранительные органы от обязанности получать судебное предписание на их сбор [22].

В тоже время историческое решение по делу «Карпентер против Соединенных Штатов» (2018) [23] ограничило спецслужбам США осуществление тотального автоматизированного анализа больших массивов данных. Верховный суд определил как грубое нарушение приватности сбор и обобщение цифровой информацию о лице. Данный судебный прецедент напрямую ограничил тотальный автоматизированный анализ больших массивов данных со стороны государства без надлежащего судебного контроля.

В Европейском Союзе регулирование носит более императивный, личностно-центрированный характер и опирается на Общий регламент по защите данных [24]. В европейской доктрине сам факт нахождения персональных данных в открытом доступе в сети Интернет (например, в профессиональных социальных сетях) не означает возможности их беспрепятственного извлечения методами OSINT. Субъекты корпоративной безопасности или органы правопорядка обязаны доказать наличие законного основания для обработки данных, а также строго соблюсти принцип ограничения целей, что накладывает существенные нормативные ограничения на функционирование автоматизированных OSINT-платформ. Как отмечает европейский эксперт в области ИТ-права А. Сплиттгербер в своем анализе стандартов защиты данных: «При сопоставлении интересов контролера и прав субъектов данных обязательно учитываются их разумные ожидания. В число ключевых факторов входят: "сдерживающий эффект" неизбирательного сбора данных на свободу выражения мнений; практическая сложность осуществления прав после сбора информации; техническая невозможность удаления персональных данных из обученной модели; а также разумные ожидания субъектов, основанные на характере исходного веб-сайта и установленных технических ограничениях» [25].

В правовой архитектуре Китая сформировалась третья, уникальная глобальная модель регулирования больших данных (Big Data) и OSINT. Если подход США можно назвать рыночно-прецедентным (защита от государства через суды), а подход ЕС — личностно-центрированным (защита прав человека через жесткий регламент GDPR), то модель КНР является государственно-центрированной. Исследователь Ф. Декаролис отмечает, что «первоначально КНР развивала цифровую сферу по американской рыночной модели, однако затем изменила вектор, переняв жесткие стандарты ЕС по ключевым правовым аспектам. Сегодня Пекин внедрил всеобъемлющее законодательство о конфиденциальности, которое в некоторых аспектах защищает права потребителей сильнее, чем законы США. Уникальные национальные особенности делают китайскую модель самобытным глобальным игроком, способным составить конкуренцию одностороннему регуляторному влиянию Запада. Современный подход Китая строится на парадоксальном сочетании тотального государственного контроля с жесткой защитой личных данных граждан, а также на принципе цифрового суверенитета. Эта «защита данных с китайской спецификой» предопределит вектор регулирования искусственного интеллекта в самой КНР и неизбежно повлияет на будущую правовую политику США и Евросоюза» [26].

3. OSINT в оперативно-розыскной и следственной деятельности

Интеграция технологий OSINT в практику органов, осуществляющих оперативно-розыскную деятельность, актуализирует фундаментальную научно-теоретическую правовую проблему, заключающуюся в отсутствии в Федеральном законе «Об оперативно-розыскной деятельности» [27] отдельного оперативно-розыскного мероприятия (ОРМ), в полной мере отражающего специ-

фику цифрового поиска.

Деятельность органов, осуществляющих оперативно-розыскную деятельность, подчинена строгому императивному принципу публичного права, согласно которому государственным органам и должностным лицам дозволено только то, что прямо предписано законом. В развитие данного постулата Конституционный Суд РФ в Определении от 01.12.1999 № 211-О зафиксировал позицию о недопустимости расширения списка ОРМ правоприменителем, подчеркнув:"...данный Федеральный закон («Об ОРД») закрепляет исчерпывающий перечень оперативно-розыскных мероприятий, проведение которых ограничивает конституционные права граждан, и устанавливает, что этот перечень может быть изменен или дополнен только федеральным законом" [28].

Цифровизация обострила проблему законности ОРМ. Массовый парсинг персональных данных и мониторинг по открытым источникам (OSINT) без введения специального "цифрового" мероприятия напрямую нарушают запрет Конституционного Суда РФ на расширение перечня ОРМ. Так, в настоящее время оперативные сотрудники вынуждены искусственно подгонять новые интернет-технологии под классический перечень мероприятий, закрепленный в законе, что ставит под сомнение легитимность таких действий. В современной следственной и оперативно-розыскной практике методы OSINT юридически легализуются преимущественно через два смежных правовых института, конструируемых на основе статьи 6 Федерального закона № 144-ФЗ «Об оперативно-розыскной деятельности» [29]: "наведение справок" и "сбор образцов для сравнительного исследования".

Данный подход правовой интерпретации рассматривает автоматизированные поисковые запросы к открытым базам данных, парсинг социальных медиа и алгоритмический анализ метаданных как процедуру получения информации по запросу у оператора информационной системы либо из общедоступного источника. Однако классическое, догматическое понимание "наведения справок" предполагает дискретный, точечный характер обращения к конкретному держателю информации. Напротив, современный инструментарий OSINT базируется на принципах непрерывного вещательного мониторинга, фонового скрапинга и компиляции сотен разрозненных, постоянно обновляющихся веб-ресурсов. Подобная качественная трансформация сущности поисковых действий выводит автоматизированный цифровой скрининг за рамки традиционного содержания указанной нормы, превращая его в процессуальную фикцию.

Похожие проблемы возникают при адаптации оперативно-розыскного мероприятия «сбор образцов для сравнительного исследования» (п. 3 ч. 1 ст. 6 ФЗ № 144-ФЗ) к интернет-среде. В рамках этой процедуры на практике часто фиксируют цифровые профили, виртуальные аватары, особенности авторского текста или технические параметры устройств. Однако, если традиционный вещественный образец всегда автономен и существует отдельно от самого правонарушения, то в цифровой среде эта граница стирается. Так, в материальном мире отпечаток пальца, оставленный на сломанном замке, физически отделен от самого повреждения. Замок выступает следом преступления, а папиллярный узор — автономным образцом, который можно скопировать отдельно. В цифровой же среде ситуация принципиально иная. Например, системный лог-файл, зафиксировавший несанкционированный доступ, одновременно содержит в себе и сам след правонарушения (факт и время взлома), и образец для исследования (IP-адрес, сетевые идентификаторы и параметры устройства).

Собираемые данные — будь то сетевой трафик, переписка или системные логи — одновременно выполняют две разные функции. С одной стороны, они фиксируют время, способ и сам факт совершения деяния. С другой стороны, эти же файлы несут в себе индивидуальные технические характеристики и стилистические паттерны, необходимые эксперту для идентификации устройства или автора текста.

Двойственная природа информации размывает границы между ключевыми юридическими понятиями: становится невозможно четко разграничить след преступления, вещественное доказательство и образец для сравнительного исследования. Это, в свою очередь, создает правовую неопределенность при определении процессуального статуса таких объектов и порядка их изъятия.

Отдельного разграничения требует дифференциация методов OSINT и ОРМ «Получение компьютерной информации» (далее — ПКИ), введенного в ст. 6 ФЗ № 144-ФЗ. Отождествление пассивного анализа общедоступного контента с данным мероприятием является методологической ошибкой.

Правовая составляющая ПКИ ориентирована на фиксацию данных, доступ к которым ограничен законным правообладателем или программно-аппаратными средствами. Проведение данного ОРМ изначально связывалось научным сообществом с преодолением барьеров приватности и "применением определенных способов доступа к информационным источникам, содержащимся в компьютерных системах" [30].

Напротив, изучение открытого сетевого контента не сопряжено с преодолением систем защиты. Избыточное применение ПКИ к откры-

тым данным размывает назначение этого мероприятия и необоснованно возвращает правоприменителя к практике расширительного толкования ОРМ "Наведение справок".

Аналогичная, но еще более выраженный правовой барьер разделяет методы OSINT и ОРМ "Снятие информации с технических каналов связи" (СИТКС). В научной литературе обоснованно отмечается главный критерий их разграничения: временной режим и способ съема данных. Так, А. Л. Осипенко отмечает: «Если информация, передаваемая с помощью компьютерных устройств (средств связи), будет перехватываться в текущем времени, т. е. в момент ее передачи, то в этом случае необходимо проводить такое ОРМ, "снятие информации с технических каналов связи"» [31].

Таким образом, сущность СИТКС заключается именно в негласном перехвате данных в процессе их трансляции по каналам коммуникации, что прямо ограничивает конституционные права граждан на тайну переписки (ст. 23 Конституции РФ) и требует обязательного судебного решения. Напротив, методы OSINT направлены на работу со сведениями, которые уже завершили цикл передачи, обработаны и размещены в открытом цифровом пространстве (веб-страницы, публичные форумы, открытые базы данных). Пассивный сбор такого контента не связан с технологическим перехватом трафика в режиме реального времени.

Отсутствие четкого разграничения данных институтов влечет за собой риски деформации правоприменительной практики. Это выражается как в избыточном бюрократическом усложнении фиксации открытой сетевой информации, так и в создании лазеек для проведения негласных оперативно-технических мероприятий без получения необходимых судебных санкций.

Особую сложность представляет этап уголовного судопроизводства, на котором результаты разведки по открытым источникам OSINT легализуются в соответствии со ст. 89 Уголовно-процессуального кодекса Российской Федерации от 18 декабря 2001 г. № 174-ФЗ [32]. Как неоднократно указывал Конституционный Суд Российской Федерации, результаты оперативно-розыскной деятельности являются не доказательствами, а лишь сведениями, которые могут стать доказательствами только после закрепления их надлежащим процессуальным путём [33]. На практике ориентирующая информация, полученная в ходе интернет-разведки, чаще всего приобретает статус «иных документов» (ст. 84 УПК РФ) либо вещественных доказательств (ст. 81 УПК РФ). Основным уязвимым элементом в данном механизме выступает процедура верификации и процессуальной фиксации цифровой информации [34].

В отличие от традиционных материальных следов, цифровая информация, извлечённая из открытых сетевых источников, обладает повышенной уязвимостью к несанкционированному изменению. Судебная практика последовательно ужесточает стандарты проверки таких сведений. Фиксация данных исключительно посредством снимков экрана (скриншотов) оперативным сотрудником зачастую признаётся судами недостаточной [35]. Как справедливо отмечает В. В. Платонов, «при оценке скриншота суд имеет возможность проверить лишь то, что представлено на бумажном носителе, однако не может установить подлинность исходных цифровых данных и факт их возможной фальсификации» [36].

Современные стандарты доказывания предполагают развёрнутую верификацию источника, включающую ведение лог-файлов, расчёт хэш-сумм загружаемых объектов, а также составление детального протокола следственного осмотра (ст. 176, 177 УПК РФ) с обязательным указанием параметров применяемого программного обеспечения и сетевых адресов узлов связи [37]. Необходимость фиксации хэш-сумм прямо вытекает из требований ч. 3 ст. 164.1 УПК РФ, обязывающей следователя указывать в протоколе применённые технические средства, порядок их применения и полученные результаты [38]. Как отмечает И. В. Литвинова, отсутствие в уголовно-процессуальном законодательстве чётких критериев допустимости компьютерной информации, полученной за пределами следственных действий, приводит к тому, что в большинстве случаев не выполняются законодательные требования, при которых такая информация могла бы быть признана допустимым доказательством [39].

Дополнительным фактором риска выступает интенсивное развитие технологий генеративного искусственного интеллекта и синтеза медиаданных (дипфейк-технологий). Современные программные комплексы позволяют создавать аутентичные по внешним признакам, но ложные цифровые следы — фото-, видео- и аудиоматериалы — с целью имитации противоправной деятельности. В условиях, когда автоматизированные OSINT-платформы осуществляют веерный мониторинг и агрегацию данных, риск интеграции фальсифицированных сведений в оперативные материалы критически возрастает. С криминалистической точки зрения дипфейки представляют собой специфический вид подложных электронно-цифровых следов, не отражающих реальных событий [40].

Данная тенденция обусловливает необходимость обязательного назначения комплексных компьютерно-технических и фоноскопических (речеведческих) экспертиз для подтверждения подлинности и неизменности первоисточника

цифровой информации [41]. Как отмечается в научной литературе, "наиболее эффективным инструментом выявления синтетического контента является комплексная экспертиза, включающая анализ артефактов в видеопотоке, установление несоответствия мимических движений и речевого сопровождения, а также фиксацию цифровых шумов, характерных для работы алгоритмов генеративных нейросетей" [42]. При этом, как указывает Я. А. Климова, в настоящее время остро стоит проблема отсутствия устойчиво работающей технологии распознавания сгенерированного контента, что снижает эффективность экспертного исследования и может приводить к невозможности решения вопроса о подлинности дипфейка при производстве экспертизы [43].

Наиболее глубокое теоретическое противоречие на стыке конституционного и уголовно-процессуального права кроется в определении пределов ограничения конституционных прав граждан при проведении разведки по открытым источникам (OSINT) государственными органами без судебного решения. Статьи 23 и 24 Конституции Российской Федерации [44] гарантируют право на неприкосновенность частной жизни, личную и семейную тайну. Ограничение права на тайну переписки допускается исключительно на основании судебного акта (ч. 2 ст. 23 Конституции РФ).

Сторонники неограниченного применения OSINT правоохранительными органами апеллируют к тому, что информация, добровольно размещённая пользователем в сети, автоматически приобретает статус общедоступной, а значит, её сбор не может нарушать конституционные права [45]. Однако, как обоснованно отмечает Р. Ю. Кохан, подобный подход игнорирует специфику оперативно-розыскных правоотношений: использование технологий OSINT-анализа, связанное с обработкой персональных данных и мониторингом социальных сетей, в силу негласного характера ограничения прав на неприкосновенность частной жизни может осуществляться только при наличии установленных законом оснований и условий для проведения оперативно-розыскных мероприятий и специальных полномочий должностного лица [46].

Системный анализ правовых позиций Конституционного Суда Российской Федерации подтверждает этот вывод. В Постановлении от 25 мая 2021 г. № 22-П КС РФ указал, что конституционные установления о неприкосновенности частной жизни «в полной мере относятся к любой информации — независимо от места и способа её производства, передачи и распространения, включая сведения, размещаемые в информационно-телекоммуникационной сети Интернет» [47]. Таким образом, цели, методы и объёмы аккумулирования информации государством имеют принципиальное значение: сам по себе открытый характер сведений не отменяет конституционных гарантий их защиты.

Применение правоохранительными органами систем тотального распознавания лиц, автоматизированного парсинга публикаций гражданина за длительный период и выявления скрытых связей между пользователями с помощью искусственного интеллекта фактически превращает разрозненные открытые данные в системное досье на личность. Показателен пример административного спора, в рамках которого гражданка А. В. Попова оспаривала использование системы распознавания лиц в Москве и требовала удалить её биометрические данные (апелляционное определение судебной коллегии по административным делам Московского городского суда от 17.02.2020 по делу № 33а-707/2020) [48]. В жалобе истец указывала, что применение технологии без её согласия нарушает конституционные гарантии неприкосновенности частной жизни и тайны персональных данных. А. Н. Мочалов, анализируя риски цифрового профилирования, справедливо указывает, что «чем больше персональных данных о лице агрегируется и подвергается обработке, тем выше степень вмешательства в частную жизнь и величина связанного с этим риска» [49]. Такое скрытое и непрерывное профилирование фактически лишает гражданина права на «цифровое уединение» [50].

Без надлежащего судебного контроля и чётких законодательных фильтров тотальный государственный OSINT рискует трансформироваться в инструмент несанкционированного контроля за частной жизнью, что прямо противоречит фундаментальным публично-правовым принципам. Как подчёркивают Н. М. Букаев и Р. А. Исмагилов, в Российской Федерации до сих пор отсутствуют чёткие инструкции и алгоритмы по использованию технологий распознавания лиц, которые удовлетворяли бы требования общества по сохранению тайны частной жизни [51].

Проблема нуждается в нормативном урегулировании. Необходимо определить четкие границы применения новых технических методов. Устранение данного правового пробела позволит соблюсти баланс между интересами правосудия и конституционными гарантиями прав личности.

4. OSINT в системе корпоративной безопасности

Ужесточение рыночного соперничества и регуляторного давления вынуждает коммерческие организации формировать превентивные механизмы защиты активов, где центральное место отводится непрерывному мониторингу бизнес-окружения. Использование инструментов OSINT субъектами корпоративной безопасности

(службами безопасности, комплаенс-подразделениями) традиционно обосновывается необходимостью реализации принципа "должной осмотрительности" (Due Diligence) и минимизации предпринимательских рисков. В правовом поле Российской Федерации такая деятельность должна строго соответствовать балансу между интересами бизнеса и конституционными гарантиями неприкосновенности частной жизни (ст. 23, 24 Конституции РФ).

Бизнес также обязан оценивать благонадежность контрагентов для минимизации налоговых рисков в контексте ст. 54.1 Налогового кодекса РФ, предотвращения легализации доходов, полученных преступным путем, и защиты собственной коммерческой тайны.

Правовым базисом корпоративного OSINT выступают нормы информационного и гражданского законодательства, легализующие сбор общедоступных сведений из неконфиденциальных государственных реестров. Информационно-аналитическое обеспечение этой деятельности реализуется через специализированные программные платформы агрегации данных. В российской практике бизнес-анализа и комплаенса ключевыми инструментами выступают системы «СПАРК» («Интерфакс»), «Контур.Фокус», Rusprofile, CheckPerson и Seldon Basis, автоматизирующие мониторинг ЕГРЮЛ/ЕГРИП и финансовых показателей контрагентов. Для верификации судебных рисков обособленно применяется официальный ресурс «Картотека арбитражных дел». Вышеперечисленные платформы обеспечивают возможность автоматизированной агрегации и анализа общедоступных данных, что соответствует законодательным требованиям в области защиты персональных данных и информационной безопасности.

Однако ситуация меняется, когда корпоративный OSINT смещается из плоскости анализа юридических лиц в область изучения физических лиц — бенефициаров бизнеса, топ-менеджеров или кандидатов на вакантные должности. Проведение кадрового скоринга (проверка профилей в социальных сетях, анализ цифровой активности) вступает в противоречие с Федеральным законом «О персональных данных» [52]. Согласно ст. 5 и ст. 6 данного закона, любая обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Сбор информации о личной жизни кандидата в сети Интернет без его письменного согласия, даже если эта информация выложена им самим в открытый доступ, представляет собой нарушение принципа целеполагания обработки данных.

На этом фоне сотрудники корпораций сталкиваются с коллизией. Эффективное выявление внутренних и внешних угроз требует цифрового поиска, в то время как формальное соблюдение регуляторных требований существенно ограничивает глубину аналитики [53].

Для специалистов в области уголовно-правовых наук наибольший теоретический и практический интерес представляет квалификация действий сотрудников корпоративных служб безопасности (СБ), переступающих грань между легальным сбором информации и уголовно наказуемыми деяниями. В отличие от государственных правоохранительных органов, наделенных специальными публично-властными полномочиями, сотрудники частных структур действуют в статусе обычных субъектов права.

Актуальная судебно-следственная практика демонстрирует тенденцию к строгому толкованию составов преступлений против конституционных прав граждан применительно к сфере информационных технологий. В частности, сбор сотрудником службы безопасности сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия образует состав преступления, предусмотренного ст. 137 УК РФ. При этом, в соответствии с разъяснениями Пленума Верховного Суда РФ, уголовная ответственность наступает и в том случае, если аналитик собирал информацию из закрытых профессиональных сообществ или персональных блогов с ограниченным доступом [54].

Аналогичным образом судами признаются незаконными перехват трафика и чтение корпоративной почты сотрудника при отсутствии надлежащим образом оформленного локальными нормативными актами режима коммерческой тайны и согласия самого работника, что влечет риски квалификации деяния по ст. 138 УК РФ [50].

Наконец, использование специалистами частного сектора специализированного программного обеспечения для скрытого парсинга данных с сайтов конкурентов, обходящего системы технической защиты (WAF, капчи), либо авторизация в закрытых CRM-системах под чужими учетными данными подпадают под действие ст. 272 УК РФ, поскольку наличие благой цели в виде защиты экономических интересов компании не является обстоятельством, исключающим преступность деяния [55].

Наиболее острой и дискуссионной проблемой современного права является массовое использование корпоративными аналитиками массивов данных, утекших в результате хакерских атак и размещенных в Даркнете. С одной стороны, эти сведения де-факто находятся в публичном доступе, не требуют взлома со стороны аналитика и используются для выявления мошеннических схем. С другой стороны, использование таких массивов де-юре является абсолютно про-

тивоправным. Позиция судов и Роскомнадзора в этом вопросе однозначна: информация, полученная в результате преступных действий (взлома и утечки), не теряет своего конфиденциального статуса и не становится общедоступной [56].

Любое обращение корпоративного аналитика к подобным базам данных с юридической точки зрения представляет собой обработку персональных данных, полученных незаконным путем. Более того, целенаправленный скан и аккумулирование баз данных конкурентов с целью переманивания клиентов выводят деятельность СБ из рамок OSINT в сферу промышленного шпионажа. Такие действия подлежат квалификации по ст. 183 УК РФ, устанавливающей ответственность за незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну.

Следовательно, рассматриваемая коллизия требует законодательного разрешения, поскольку от выбранной модели регулирования зависит обеспечение конституционных прав граждан при применении цифровых инструментов в правоохранительной и частной детективной деятельности.

5. Заключение

Проведённое междисциплинарное исследование позволило выявить существенные нормативно-правовые проблемы в регулировании OSINT в современной России. Центральной коллизией является противоречие между государственными интересами в области национальной безопасности и правом граждан на цифровую приватность. С точки зрения публично-правовых отношений государство обязано обеспечивать безопасность и правопорядок, используя современные инструменты, включая OSINT. В условиях гибридных угроз такой мониторинг становится критически важным инструментом для выявления противоправных элементов. Частноправовые интересы бизнеса также требуют использования OSINT для защиты активов от мошеннических действий.

В то же время с позиции уголовно-правовых норм и конституционной доктрины бесконтрольный сбор и анализ цифровых данных создают риски для прав личности. Отсутствие чётких нормативных фильтров превращает OSINT в инструмент тотальной прозрачности, что противоречит принципу контроля над персональными данными. Особую актуальность приобретает проблема правового статуса динамически изменяемых интернет-данных. Юридическая практика сталкивается с вопросами о допустимости использования кэш-копий удалённых или приватных данных, а также с необходимостью разграничения профессионального и личного контента при сборе информации. Существующая правовая система характеризуется терминологическим хаосом и отсутствием чёткого регулирования OSINT. Отсутствие легальных определений понятий "цифровой поиск", "OSINT" и "скрейпинг данных" приводит к правовой неопределённости.

Исследование показало, что развитие технологий OSINT опережает модернизацию законодательной базы, что создаёт системные риски как в оперативно-розыскной деятельности, так и в корпоративной сфере. Для устранения выявленных проблем целесообразно рассмотреть введение в сфере оперативно-розыскного права нового вида оперативно-розыскного мероприятия — «цифровой поиск», а также разграничить режимы пассивного мониторинга и активного поиска. В сфере частно-публичных отношений требуется разработка под эгидой Минцифры РФ единого «Стандарта легитимного использования открытых данных в комплаенс-мониторинге» с одновременным запретом для коммерческих структур использовать данные, полученные из утечек.

В сфере правоприменения необходимо регламентировать порядок признания допустимости OSINT-материалов в качестве доказательств, определить процессуальные критерии их использования, включая обязательную фиксацию хэш-сумм файлов и логирование сетевого трафика, а также установить правила обращения с кэш-копиями удалённых данных. Ключевой вывод исследования заключается в необходимости формирования новой парадигмы правового регулирования OSINT, базирующейся на характере, целях и масштабах автоматизированной обработки данных. Модернизация законодательной базы должна обеспечить сбалансированное сочетание государственных интересов, потребностей бизнеса и гарантий прав граждан на цифровую приватность.

Список литературы:

[1] Global Datasphere to Hit 175 Zettabytes by 2025, IDC Says // Big Data Wire / HPCwire. — 2018. — 27 Nov. — URL: hpcwire.com (дата обращения: 01.09.2026).

[2] Исаков В. Б. Правовая аналитика и автоматизированные системы в юриспруденции // Право и цифровая экономика. 2024. № 2. С. 15–28. DOI: 10.17323/2712-8172-2024-2-15-28. URL: https://law-journal.hse.ru/.

[3] Хабриева Т. Я. Право в условиях цифровизации [Текст] / Талия Хабриева. - Санкт-Петербург : СПбГУП, 2019. - 27 с., [2] л. цв. ил., портр. - (Избранные лекции Университета ; вып. 189). - 500 экз. - ISBN 978-5-7621-1011-2.

[4] Тихомиров Ю. А., Кичигин Н. В., Цомартова Ф. В., Бальхаева С. Б. Право и цифровая трансформация // Право. Журнал Высшей школы экономики. — 2021. — № 2. — С. 4–23.

[5] Цифровое право : учебник / под общ. ред. В. В. Блажеева, М. А. Егоровой. — 2-е изд., перераб. и доп. — Москва : Проспект, 2025. — 848 с. — ISBN 978-5-392-43355-1.

[6] Информационные технологии в юридической деятельности: правовая информатика, информационное и цифровое право : учебник для вузов / М. В. Воронин, Е. А. Ильюшин, В. Ю. Патенкова [и др.] ; под ред. В. А. Вайпана ; Московский государственный университет имени М. В. Ломоносова, Юридический факультет. – Москва: Юстицинформ, 2024. – 752 с. – ISBN 978-5-7205-2015-1.

[7] Архипов, В. В. Интернет-право : учебник для вузов / В. В. Архипов. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2026. – 254 с. – (Высшее образование). – ISBN 978-5-534-19047-2.

[8] Виноградов В. А., Кузнецова Д. В. Зарубежный опыт правового регулирования технологии «дипфейк» // Право. Журнал Высшей школы экономики. 2024. Том 17. № 2. С. 220. DOI: 10.17323/2072-8166.2024.2.215.240.

[9] Богдановская И. Ю., Васякина Е. В., Волос А. А., Данилов Н. А., Егорова Е. В., Калятин В. О., Карпенко О. И., Салихов Д. Р. Искусственный интеллект и право // Право. Журнал Высшей школы экономики. 2024. Том 17. № 4. С. 278–306. DOI: 10.17323/2072-8166.2024.4.278.306.

[10] Правовое регулирование цифровых технологий в России и за рубежом. Роль и место правового регулирования и саморегулирования в развитии цифровых технологий: монография / под общей редакцией А. В. Минбалеева. — Саратов: Амирит, 2019. — 207 с. — ISBN 978-5-00140-394-4. — Текст : непосредственный.

[11] Кузнецов П. У. Информационное право : учебник для студентов высших учебных заведений, обучающихся по направлению и специальности «Юриспруденция» / П. У. Кузнецов ; Уральский государственный юридический университет. — Москва : Юстиция ; Екатеринбург : Издательство Уральского государственного юридического университета, 2022. — 335 с. — (Серебряная серия) (Бакалавриат) (ФГОС). — ISBN 978-5-4365-3905-8. — Текст : непосредственный.

[12] Филипова И. А. Правовое регулирование искусственного интеллекта : учебное пособие / И. А. Филипова ; Национальный исследовательский Нижегородский государственный университет им. Н. И. Лобачевского. — 3-е изд., перераб. и доп. — Нижний Новгород: Нижегородский госуниверситет, 2025. — 321 с. — Текст: непосредственный.

[13] Воскобитова Л. А. Уголовное судопроизводство: трансформация теоретических представлений и регулирования в условиях цифровизации : монография / Л. А. Воскобитова, В. И. Пржиленский. — Москва : Норма : ИНФРА-М, 2022. — 288 с. — ISBN 978-5-00156-259-7. — Текст : непосредственный.

[14] Расторопов С. В., Прорвич В. А. Информационные основы современной уголовно-правовой защиты субъектов цифровой экономики и финансов // Право. Журнал Высшей школы экономики. 2024. Т. 17. № 2. С. 143–169.

[15] Янгаева М. О. OSINT. Получение криминалистически значимой информации из сети Интернет / М. О. Янгаева, Н. О. Павленко // Алтайский юридический вестник. — 2022. — № 2 (38). — С. 131–135. — DOI 10.24412/2224-9133-2022-2-131-135. — URL: https://cyberleninka.ru/article/n/osint-poluchenie-kriminalisticheski-znachimoy-informatsii-iz-seti-internet (дата обращения: 04.09.2026).

[16] О персональных данных : Федеральный закон № 152-ФЗ : [принят Государственной Думой 8 июля 2006 года : одобрен Советом Федерации 14 июля 2006 года] // Официальный интернет-портал правовой информации. — URL: pravo.gov.ru (дата обращения: 04.09.2026).

[17] Уголовный кодекс Российской Федерации : Федеральный закон № 63-ФЗ : [принят Государственной Думой 24 мая 1996 года : одобрен Советом Федерации 5 июня 1996 года] // Официальный интернет-портал правовой информации. — URL: pravo.gov.ru (дата обращения: 04.09.2026).

[18] О персональных данных : Федеральный закон № 152-ФЗ : [принят Государственной Думой 8 июля 2006 года : одобрен Советом Федерации 14 июля 2006 года] // Официальный интернет-портал правовой информации. — URL: pravo.gov.ru (дата обращения: 04.09.2026).

[19] Виноградов В. А., Кузнецова Д. В. Зарубежный опыт правового регулирования технологии «дипфейк» // Право. Журнал Высшей школы экономики. 2024. Том 17. № 2. С. 220. DOI: 10.17323/2072-8166.2024.2.215.240.

[20] Burnham W. (2006). Introduction to the Law and Legal System of the United States (4th ed.). St. Paul, MN: West Academic Publishing. ISBN: 978-0314158987. URL: https://archive.org/details/introductiontola0000burn.

[21] Katz v. United States: judgment of the Supreme Court of the United States, Dec. 18, 1967 // United States Reports. — 1967. — Vol. 389. — P. 347.

[22] Supreme Court of the United States. Carpenter v. United States, 138 S. Ct. 2206 (2018); Katz v. United States, 389 U.S. 347 (1967) // Supreme Court Reports. — URL: supremecourt.gov.

[23] Carpenter v. United States: judgment of the Supreme Court of the United States, June 22, 2018 // United States Reports. — 2018. — Vol. 138. — P. 2206.

[24] European Data Protection Board (EDPB).

Guidelines 08/2020 on the targeting of social media users. — Brussels, 2021. — 45 p. — URL: europa.eu (дата обращения: 08.09.2026).

[25] Splittgerber A. EDPB web scraping guidelines for AI: Making the impossible possible? / A. Splittgerber // Technology Law Dispatch (Reed Smith LLP). — July 2026. — URL: https://www.reedsmith.com/our-insights/blogs/technology-law-dispatch/102nbqu/edpb-web-scraping-guidelines-for-ai-making-the-impossible-possible/..

[26] Wang G. China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU / G. Wang, E. Kosta // Tilburg Law School Legal Studies Research Paper Series. — 2023. — № 04. — 32 p. — URL: ssrn.com (дата обращения: 03.09.2026).

[27] Об оперативно-розыскной деятельности : Федеральный закон от 12.08.1995 № 144-ФЗ (последняя редакция) // Собрание законодательства Российской Федерации. – 1995. – № 33. – Ст. 3349.

[28] Определение Конституционного Суда РФ от 01.12.1999 № 211-О «Об отказе в принятии к рассмотрению жалобы гражданина Барковского Константина Олеговича на нарушение его конституционных прав частью четвертой статьи 127 УПК РСФСР, пунктом 1 части первой статьи 6 и пунктом 3 части первой статьи 7 Федерального закона "Об оперативно-розыскной деятельности"» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_26657/ (дата обращения: 08.09.2026).

[29] Об оперативно-розыскной деятельности: Федеральный закон от 12.08.1995 № 144-ФЗ (последняя редакция) // Собрание законодательства Российской Федерации. – 1995. – № 33. – Ст. 3349.

[30] Гердт К.М., Поляков В.В. Получение компьютерной информации: понятие, содержание и особенности производства оперативно-розыскного мероприятия // Проблемы правовой и технической защиты информации. — 2019. — № 7. — С. 71–75.

[31] Осипенко А. Л. [и др.] Алгоритм реализации оперативно-розыскного мероприятия «получение компьютерной информации» при выявлении, предупреждении, пресечении и раскрытии преступлений экстремистской направленности и террористического характера: методические рекомендации. — Краснодар: Краснодарский ун-т МВД России, 2019. — ISBN 978-5-9266-1525-5.

[32] Галузо В. Н., Фетищев Д. В., Соломин Д. А. Легализация результатов оперативно-розыскной деятельности в уголовном процессе Российской Федерации: монография. – М. : Проспект, 2025. – 368 с.

[33] Определение Конституционного Суда РФ от 04.02.1999 № 18-О «По жалобе граждан М. Б. Никольского и М. И. Сапронова на нарушение их конституционных прав отдельными положениями Федерального закона "Об оперативно-розыскной деятельности"» // Вестник Конституционного Суда РФ. — 1999. — № 3.

[34] Литвинова И. В. Проблемы допустимости электронных доказательств, полученных при производстве иных процессуальных действий // Российский юридический журнал. – 2023. – № 1. – С. 139–147.

[35] Платонов В. В. Обеспечение допустимости электронных доказательств в уголовном судопроизводстве // Актуальные проблемы российского права. – 2025. – Т. 20, № 8 (177). – С. 124–132. – DOI: 10.17803/1994-1471.2025.177.8.124-132..

[36] Платонов В. В. Указ. соч. – С. 128.

[37] Константинов А. В., Поликарпова Е. В. Допустимость электронных доказательств, полученных в результате поисково-познавательной деятельности в сети Интернет // Экономика. Право. Общество. – 2025. – Т. 10, № 4. – С. 141–145. – DOI: 10.21686/2411-118X-2025-4-141-145..

[38] Нисневич А. К. OSINT-анализ сайтов как метод сбора доказательств по уголовным делам // Вестник Белгородского юридического института МВД России имени И. Д. Путилина. – 2026. – № 2. – С. 98–105.

[39] Литвинова И. В. Проблемы допустимости электронных доказательств, полученных при производстве иных процессуальных действий // Российский юридический журнал. – 2023. – № 1. – С. 142.

[40] Поляков В. В. Применение дипфейк-технологий при совершении высокотехнологичных преступлений // Lex russica. – 2026. – Т. 79, № 8. – С. 85–95. – DOI: 10.17803/1729-5920.2026.237.8.085-095..

[41] Асадов Р. Б. Цифровая мимикрия: защита прав личности от противоправного применения дипфейк-технологий // Полицейская и следственная деятельность. – 2025. – № 4. – С. 16–36. – DOI: 10.25136/2409-7810.2025.4.75462..

[42] Захарцев С. И., Тамодин Н. В., Чумаевская Е. Б. Дипфейки и способы их выявления: вопросы криминалистики // Образование. Наука. Научные кадры. – 2026. – № 2. – С. 199–207.

[43] Климова Я. А. Основные положения частной криминалистической методики расследования преступлений, совершённых с использованием технологии дипфейк: от теории к практике киберследствия // Актуальные проблемы российского права. – 2025. – Т. 20, № 10 (179). – С. 133–143. – DOI: 10.17803/1994-1471.2025.179.10.133-143..

[44] Конституция Российской Федерации : принята всенародным голосованием 12 дек.

1993 г. (с изм., одобренными в ходе общероссийского голосования 1 июля 2020 г.) // Официальный интернет-портал правовой информации. URL: (дата обращения: 08.09.2026).

[45] Тарасов А. А. Уголовно-правовые аспекты использование методов OSINT // Право и управление. – 2026. – № 8. – С. 234–241.

[46] Кохан Р. Ю. О проблемных вопросах обеспечения конституционных прав граждан в процессе информационно-аналитического обеспечения оперативно-розыскной деятельности, использования технологий OSINT-анализа // Вестник Сибирского юридического института МВД России. – 2024. – № 4 (57). – С. 87–94.

[47] Постановление Конституционного Суда Российской Федерации от 25 мая 2021 г. № 22-П «По делу о проверке конституционности пункта 8 части 1 статьи 6 Федерального закона "О персональных данных" в связи с жалобой общества с ограниченной ответственностью "МедРейтинг"» // Официальный интернет-портал правовой информации. URL: (дата обращения: 08.09.2026).

[48] Апелляционное определение судебной коллегии по административным делам Московского городского суда от 17.02.2020 по делу № 33а-707/2020.

[49] Мочалов А. Н. Цифровой профиль: основные риски для конституционных прав человека в условиях правовой неопределенности // Lex russica. – 2021. – Т. 74, № 9. – С. 88–101. – DOI: 10.17803/1729-5920.2021.178.9.088-101..

[50] Мочалов А. Н. Указ. соч. – С. 95.

[51] Букаев Н. М., Исмагилов Р. А. К вопросу соблюдения конституционных прав граждан в уголовном судопроизводстве при использовании в доказывании камер с функцией распознавания лиц // Вестник Уральского юридического института МВД России. – 2021. – № 1. – С. 81–85.

[52] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства РФ. – 2006. – № 31 (ч. 1). – Ст. 3451.

[53] Мочалов А. Н. Цифровой профиль: основные риски для конституционных прав человека в условиях правовой неопределенности // Lex russica. – 2021. – Т. 74, № 9 (178). – С. 89.

[54] Постановление Пленума Верховного Суда РФ от 25.12.2018 № 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина» // Бюллетень Верховного Суда РФ. – 2019. – № 2.

[55] Букаев Н. М., Исмагилов Р. А. К вопросу соблюдения конституционных прав граждан в уголовном судопроизводстве при использовании в доказывании камер с функцией распознавания лиц // Вестник Уральского юридического института МВД России. – 2021. – № 1. – С. 83.

[56] Доклад об итогах деятельности Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций за 2023 год // Официальный сайт Роскомнадзора. — 2024. — URL: https://rkn.gov.ru (дата обращения: 08.09.2026).

References:

[1] Global Datasphere to Hit 175 Zettabytes by 2025, IDC Says // Big Data Wire / HPCwire. — 2018. - 27 Nov - URL: hpcwire.com (accessed on: 01.09.2026).

[2] Isakov V. B. Legal Analytics and Automated Systems in Jurisprudence // Law and the Digital Economy. 2024. № 2. S. 15-28. DOI: 10.17323/2712-8172-2024-2-15-28. URL: https://law-journal.hse.ru/.

[3] Khabrieva T. Ya. Law in the context of digitalization [Text]/Taliya Khabrieva. - St. Petersburg: SPbGUP, 2019. - 27 s., [2] l. zv. il., portr. - (Selected lectures of the University; issue 189). - 500 copies - ISBN 978-5-7621-1011-2.

[4] Tikhomirov Yu. A., Kichigin N. V., Tsomartova F. V., Balkhaeva S. B. Law and digital transformation // Law. Journal of the Higher School of Economics. — 2021. — № 2. - S. 4-23.

[5] Digital law: textbook/under the general. ed. V.V. Blazheeva, M.A. Egorova. - 2nd ed., Revised and add. - Moscow: Prospect, 2025. - 848 p. - ISBN 978-5-392-43355-1.

[6] Information technologies in legal activities: legal informatics, information and digital law: a textbook for universities/M. V. Voronin, E. A. Ilyushin, V. Yu. Patenkova [and others]; ed. V. A. Vaipana; Lomonosov Moscow State University, Faculty of Law. - Moscow: Justicinform, 2024. - 752 p. - ISBN 978-5-7205-2015-1.

[7] Arkhipov, V.V. Internet law: a textbook for universities/V.V. Arkhipov. - 2nd ed., Revised and add. - Moscow: Yurayt Publishing House, 2026. - 254 p. - (Higher education). – ISBN 978-5-534-19047-2.

[8] Vinogradov V. A., Kuznetsova D. V. Foreign experience in the legal regulation of deepfake technology // Law. Journal of the Higher School of Economics. 2024. Volume 17. № 2. S. 220. DOI: 10.17323/2072-8166.2024.2.215.240.

[9] Bogdanovskaya I. Yu., Vasyakina E.V., Volos A.A., Danilov N.A., Egorova E.V., Kalyatin V.O., Karpenko O.I., Salikhov D.R. Artificial intelligence and law // Law. Journal of the Higher School of Economics. 2024. Volume 17. № 4. S. 278-306. DOI: 10.17323/2072-8166.2024.4.278.306.

[10] Legal regulation of digital technologies in Russia and abroad. The role and place of legal regulation and self-regulation in the development of digital technologies: monograph/under the general editorship of A. V. Minbaleev. - Saratov: Amirit, 2019. - 207 p. - ISBN 978-5-00140-394-4. - Text: direct.

[11] Kuznetsov P.U. Information Law: a textbook for students of higher educational institutions studying in the direction and specialty "Jurisprudence "/P.U. Kuznetsov; Ural State Law University. - Moscow: Justice; Yekaterinburg: Publishing House of the Ural State Law University, 2022. - 335 p. - (Silver series) (Undergraduate) (GEF). — ISBN 978-5-4365-3905-8. - Text: direct.

[12] Filipova I. A. Legal regulation of artificial intelligence: a textbook/I. A. Filipova; National Research Nizhny Novgorod State University named after N.I. Lobachevsky. - 3rd ed., Revised and add. - Nizhny Novgorod: Nizhny Novgorod State University, 2025. - 321 p. - Text: direct.

[13] Voskobitova L. A. Criminal proceedings: transformation of theoretical ideas and regulation in conditions of digitalization: monograph/ L. A. Voskobitova, V. I. Przhilensky. - Moscow: Norm: INFRA-M, 2022. - 288 p. - ISBN 978-5-00156-259-7. - Text: direct.

[14] Rastoropov S.V., Prorvich V.A. Information foundations of modern criminal legal protection of subjects of the digital economy and finance // Law. Journal of the Higher School of Economics. 2024. VOL. 17. № 2. S. 143-169.

[15] M.O. Yangaeva OSINT. Obtaining criminally significant information from the Internet/ M. O. Yangaeva, N. O. Pavlenko // Altai Legal Bulletin. — 2022. — № 2 (38). - S. 131-135. — DOI 10.24412/2224-9133-2022-2-131-135. — URL: https://cyberleninka.ru/article/n/osint-poluchenie-kriminalisticheski-znachimoy-informatsii-iz-seti-internet (дата обращения: 04.09.2026).

[16] On personal data: Federal Law No. 152-FZ: [adopted by the State Duma on July 8, 2006: approved by the Federation Council on July 14, 2006] // Official Internet portal of legal information. - URL: pravo.gov.ru (access date: 04.09.2026).

[17] Criminal Code of the Russian Federation: Federal Law No. 63-FZ: [adopted by the State Duma on May 24, 1996: approved by the Federation Council on June 5, 1996] // Official Internet portal of legal information. - URL: pravo.gov.ru (access date: 04.09.2026).

[18] On personal data: Federal Law No. 152-FZ: [adopted by the State Duma on July 8, 2006: approved by the Federation Council on July 14, 2006] // Official Internet portal of legal information. - URL: pravo.gov.ru (access date: 04.09.2026).

[19] Vinogradov V. A., Kuznetsova D. V. Foreign experience in the legal regulation of deepfake technology // Law. Journal of the Higher School of Economics. 2024. Volume 17. № 2. S. 220. DOI: 10.17323/2072-8166.2024.2.215.240.

[20] Burnham W. (2006). Introduction to the Law and Legal System of the United States (4th ed.). St. Paul, MN: West Academic Publishing. ISBN: 978-0314158987. URL: https://archive.org/details/introductiontola0000burn.

[21] Katz v. United States: judgment of the Supreme Court of the United States, Dec. 18, 1967 // United States Reports. — 1967. — Vol. 389. — P. 347.

[22] Supreme Court of the United States. Carpenter v. United States, 138 S. Ct. 2206 (2018); Katz v. United States, 389 U.S. 347 (1967) // Supreme Court Reports. — URL: supremecourt.gov.

[23] Carpenter v. United States: judgment of the Supreme Court of the United States, June 22, 2018 // United States Reports. — 2018. — Vol. 138. — P. 2206.

[24] European Data Protection Board (EDPB). Guidelines 08/2020 on the targeting of social media users. — Brussels, 2021. — 45 p. - URL: europa.eu (access date: 08.09.2026).

[25] Splittgerber A. EDPB web scraping guidelines for AI: Making the impossible possible? / A. Splittgerber // Technology Law Dispatch (Reed Smith LLP). — July 2026. — URL: https://www.reedsmith.com/our-insights/blogs/technology-law-dispatch/102nbqu/edpb-web-scraping-guidelines-for-ai-making-the-impossible-possible/..

[26] Wang G. China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU / G. Wang, E. Kosta // Tilburg Law School Legal Studies Research Paper Series. — 2023. — № 04. — 32 p. - URL: ssrn.com (access date: 03.09.2026).

[27] On operational-search activities: Federal Law of 12.08.1995 No. 144-FZ (latest edition) // Collection of legislation of the Russian Federation. – 1995. – № 33. - Art. 3349.

[28] Determination of the Constitutional Court of the Russian Federation of 01.12.1999 No. 211-O "On refusal to accept for consideration the complaint of citizen Barkovsky Konstantin Olegovich about violation of his constitutional rights by part four of article 127 of the Code of Criminal Procedure of the RSFSR, paragraph 1 of part one of article 6 and paragraph 3 of part one of article 7 of the Federal Law "On operational-search activities" "// SPS" ConsultantPlus. "URL: https://www.consultant.ru/document/cons_doc_LAW_26657/ (access date: 08.09.2026).

[29] On operational-search activities: Federal Law of 12.08.1995 No. 144-FZ (latest edition) // Collection of legislation of the Russian Federation. – 1995. – № 33. - Art. 3349.

[30] Gerdt K.M., Polyakov V.V. Obtaining computer information: the concept, content and features of the production of operational-search measures // Problems of legal and technical protection of information. — 2019. — № 7. - S. 71-75.

[31] Osipenko A. L. [et al.] Algorithm for the implementation of the operational-search measure "obtaining computer information" in the identification, prevention, suppression and

disclosure of crimes of an extremist and terrorist nature: guidelines. - Krasnodar: Krasnodar University of the Ministry of Internal Affairs of Russia, 2019. — ISBN 978-5-9266-1525-5.

[32] Galuso V.N., Fetishchev D.V., Solomin D.A. Legalization of the results of operational-search activities in the criminal process of the Russian Federation: monograph. - M.: Prospect, 2025. - 368 p.

[33] Determination of the Constitutional Court of the Russian Federation of 04.02.1999 No. 18-O "On the complaint of citizens M. B. Nikolsky and M. I. Sapronov about violation of their constitutional rights by certain provisions of the Federal Law "On Operational-Search Activities" "// Bulletin of the Constitutional Court of the Russian Federation. — 1999. — № 3.

[34] Litvinova I.V. Problems of admissibility of electronic evidence obtained in the course of other procedural actions // Russian Law Journal. – 2023. – № 1. - S. 139-147.

[35] Platonov V. V. Ensuring the admissibility of electronic evidence in criminal proceedings // Actual problems of Russian law. – 2025. - T. 20, NO. 8 (177). - S. 124-132. – DOI: 10.17803/1994-1471. 2025.177.8.124-132..

[36] Platonov V.V. Decree. Op. - S. 128.

[37] Konstantinov A.V., Polikarpova E.V. Admissibility of electronic evidence obtained as a result of search and cognitive activity on the Internet // Economics. Right. Society. – 2025. - T. 10, NO. 4. - S. 141-145. – DOI: 10.21686/2411-118X-2025-4-141-145..

[38] Nisnevich A.K. OSINT-analysis of sites as a method of collecting evidence in criminal cases // Bulletin of the Belgorod Law Institute of the Ministry of Internal Affairs of Russia named after I.D. Putilin. – 2026. – № 2. - S. 98-105.

[39] Litvinova I.V. Problems of admissibility of electronic evidence obtained in the course of other procedural actions // Russian Law Journal. – 2023. – № 1. - S. 142.

[40] Polyakov V.V. The use of deepfake technologies in the commission of high-tech crimes // Lex russica. – 2026. - T. 79, NO. 8. - S. 85-95. – DOI: 10.17803/1729-5920.2026.237.8.085-095..

[41] Asadov R. B. Digital mimicry: protection of individual rights from illegal use of deepfake technologies // Police and investigative activities. – 2025. – № 4. - S. 16-36. – DOI: 10.25136/2409-7810. 2025.4.75462..

[42] Zakhartsev S.I., Tamodin N.V., Chumaevskaya E.B. Deepfeyki and ways to identify them: forensic issues // Education. Science. Scientific cadres. – 2026. – № 2. - S. 199-207.

[43] Klimova Ya. A. The main provisions of the private forensic methodology for investigating crimes committed using deepfake technology: from theory to practice of cyber investigation // Actual problems of Russian law. – 2025. - T. 20, NO. 10 (179). - S. 133-143. – DOI: 10.17803/1994-1471.2025.179.10. 133-143..

[44] Constitution of the Russian Federation: adopted by popular vote on December 12, 1993 (with amendments approved during the all-Russian vote on July 1, 2020) // Official Internet portal of legal information. URL: (access date: 08.09.2026).

[45] Tarasov A. A. Criminal law aspects use of OSINT methods // Law and management. – 2026. – № 8. - S. 234-241.

[46] Kohan R. Yu. On problematic issues of ensuring the constitutional rights of citizens in the process of information and analytical support of operational-search activities, the use of OSINT-analysis technologies // Bulletin of the Siberian Law Institute of the Ministry of Internal Affairs of Russia. – 2024. – № 4 (57). - S. 87-94.

[47] Decision of the Constitutional Court of the Russian Federation of May 25, 2021 No. 22-P "In the case of checking the constitutionality of paragraph 8 of part 1 of Article 6 of the Federal Law" On Personal Data "in connection with the complaint of the MedRating limited liability company "// Official Internet portal of legal information. URL: (access date: 08.09.2026).

[48] Appellate Ruling of the Administrative Court of the Moscow City Court dated 17.02.2020 in case No. 33a-707/2020.

[49] Mochalov A. N. Digital profile: the main risks for constitutional human rights in conditions of legal uncertainty // Lex russica. – 2021. - T. 74, NO. 9. - S. 88-101. – DOI: 10.17803/1729-5920.2021.178.9. 088-101..

[50] Mochalov A.N. Decree. Op. - S. 95.

[51] Bukaev N. M., Ismagilov R. A. On the issue of observing the constitutional rights of citizens in criminal proceedings when using cameras with face recognition function in evidence // Bulletin of the Ural Law Institute of the Ministry of Internal Affairs of Russia. – 2021. – № 1. - S. 81-85.

[52] Federal Law of 27.07.2006 No. 152-FZ "On Personal Data "// Collection of Legislation of the Russian Federation. – 2006. - No. 31 (part 1). - Art. 3451.

[53] Mochalov A. N. Digital profile: the main risks for constitutional human rights in conditions of legal uncertainty // Lex russica. – 2021. - T. 74, NO. 9 (178). - S. 89.

[54] Resolution of the Plenum of the Supreme Court of the Russian Federation of 25.12.2018 No. 46 "On some issues of judicial practice in cases of crimes against constitutional rights and freedoms of man and citizen "// Bulletin of the Supreme Court of the Russian Federation. – 2019. – № 2.

[55] Bukaev N. M., Ismagilov R. A. On the issue of compliance with the constitutional rights of

citizens in criminal proceedings when using cameras with face recognition function in evidence // Bulletin of the Ural Law Institute of the Ministry of Internal Affairs of Russia. – 2021. – № 1. - S. 83.

[56] Report on the results of the activities of the Federal Service for Supervision of Communications, Information Technology and Mass Communications for 2023 // Official website of Roskomnadzor. — 2024. - URL: https://rkn.gov.ru (access date: 08.09.2026).

