УДК 343.9

ПРЕДЕЛЫ И ВОЗМОЖНОСТИ КРИМИНАЛИСТИЧЕСКОЙ ИДЕНТИФИКАЦИИ В УСЛОВИЯХ МАССОВОЙ ЦИФРОВИЗАЦИИ

Колубкова А.А. [1]

студент,

кафедра юриспруденции

Институт истории и права

Калужский государственный университет им. К.Э. Циолковского

Калуга, Россия

Шейхутдинова Д.С.

студент,

кафедра юриспруденции

Институт истории и права

Калужский государственный университет им. К.Э. Циолковского

Калуга, Россия

Аннотация: В статье исследуется трансформация классических принципов и методов криминалистической идентификации под влиянием процессов массовой цифровизации. Авторы анализируют расширение объектов и средств идентификации за счет цифровых следов, рассматривают новые возможности, предоставляемые технологиями больших данных, искусственным интеллектом и биометрией, а также выявляют принципиальные пределы и риски, связанные с вероятностным характером алгоритмических выводов, проблемой цифрового дуализма и правовыми коллизиями. Делается вывод о необходимости адаптации теоретической базы криминалистической идентификации к условиям физическо-цифровой реальности, разработки новых стандартов достоверности и законодательного закрепления процедур верификации автоматизированных решений.

[1] Научный руководитель – Дроздов Д.Е., к.ю.н., доцент, Калужский государственный университет им. К.Э. Циолковского

Ключевые слова: криминалистическая идентификация, цифровизация, цифровой след, искусственный интеллект, большие данные, биометрия, достоверность, доказательственное значение.

LIMITS AND POSSIBILITIES OF CRIMINALISTIC IDENTIFICATION IN THE CONTEXT OF MASS DIGITALIZATION

Kolubkova A.A [2]

Student,

Department of Jurisprudence Institute of History and Law

Kaluga State University named after K.E. Tsiolkovsky

Kaluga, Russia

Sheikhutdinova D.S.

Student,

Department of Jurisprudence Institute of History and Law

Kaluga State University named after K.E. Tsiolkovsky

Kaluga, Russia

Abstract: The article explores the transformation of classical principles and methods of forensic identification under the influence of mass digitalization processes. The authors analyze the expansion of objects and means of identification through digital traces, examine the new opportunities provided by big data technologies, artificial intelligence, and biometrics, and identify the fundamental limits and risks associated with the probabilistic nature of algorithmic conclusions, the problem of digital dualism, and legal conflicts. The article concludes that it is necessary to adapt the theoretical framework of forensic identification to the conditions of physical and digital reality, develop new standards of reliability, and establish legal procedures for verifying automated solutions.

Keywords: forensic identification, digitalization, digital footprint, artificial intelligence, big data, biometrics, reliability, and evidential value.

[2] Scientific Supervisor: Drozdov D.E., PhD in Law, Associate Professor, Kaluga State University named after K.E. Tsiolkovsky

Настоящее исследование обусловлено высокой актуальностью, порожденной процессами тотальной цифровизации, которые фундаментально трансформируют парадигму криминалистической идентификации. Классический объектный ряд, ограниченный преимущественно материальными следами, претерпевает стремительное расширение круга объектов, включая принципиально новые, нематериальные следы. Параллельно происходит кардинальная смена методологической основы: традиционные пороговые модели, ориентированные на достижение категоричного вывода о тождестве, вытесняются вероятностно-статистическими подходами, характерными для систем искусственного интеллекта и анализа больших данных. Это объективное развитие создает ситуацию теоретического разрыва**,** когда практика опережает устоявшиеся доктринальные конструкции**,** что настоятельно требует критического переосмысления и модернизации самих концептуальных основ учения об идентификации.

Классическая теория криминалистической идентификации, сформулированная в трудах С. М. Потапова, В. Я. Колдина, Н. П. Яблокова, традиционно опиралась на материальные, статичные следы-отображения, оставляемые в физическом мире, и предполагала категоричный вывод о тождестве индивидуально-определенного объекта [1, с. 109]. Однако эпоха массовой цифровизации, характеризующаяся опосредованием человеческой деятельности информационными системами, формированием «цифровых двойников» и автоматизированным анализом информации, противостоит этим устоявшимся парадигмам.

Цифровизация меняет классическую дихотомию «идентифицируемый объект – идентифицирующий след». Цифровизация искажает старое жёсткое противопоставление, где было только два понятия: “объект, который ищут” и “след, который он оставил”. Теперь всё сложнее — объекты и следы

смешиваются, появилось третье, что еще не нашло своего отражения в теории криминалистической идентификации. Во-первых, сам цифровой след (совокупность данных, отражающих событие или действие в информационной системе) становится универсальным объектом идентификации. Следы в киберпространстве обладают свойствами виртуальности, копируемости, трансформируемости и глобальной распространенности, что принципиально меняет работу с ними. Как отмечает В. А. Мещеряков, виртуальные следы, представляя собой зафиксированные компьютерные изменения информационной системы, связанные с преступлением, не могут быть однозначно отнесены ни к материальным, ни к идеальным. Эта концепция помещает их в условно промежуточное положение, предлагая тем самым решение для классификации новых цифровых феноменов [2, с. 33].

Во-вторых, возникает ряд новых видов идентификации, не укладывающихся в традиционную классификацию, например, необходимость идентификации цифрового субъекта. Цифровой профиль личности превратился в обязательный инструмент для совершения практически любых значимых действий в интернет-пространстве. Задача состоит в установлении тождества цифрового профиля, программного агента (бота) или аккаунта в различных системах. Криминалистический анализ нацелен на подтверждение того, что конкретный цифровой профиль, программный агент или аккаунт в одной системе принадлежит тому же субъекту (или контролируется тем же оператором), что и его корреляты в других информационных пространствах. Как подчеркивают В.Б. Вехов и С.В. Зуев, эволюция криминалистической науки в условиях формирования цифрового пространства, изучает закономерности работы с цифровыми данными и средствами их обработки в контексте борьбы с правонарушениями. Результатом этого изучения является разработка технических, тактических и методических инструментов,

направленных на оптимизацию деятельности по выявлению, раскрытию, расследованию и предупреждению преступлений [3, с. 7].

Также, идентификация устройства (источника цифровых следов) – направление, активно развиваемое в рамках компьютерно-технической экспертизы (Е.Р. Россинская), которое предполагает установление индивидуальной совокупности признаков аппаратного и программного обеспечения, оставляемых при взаимодействии с сетью или носителем информации. В качестве объектов теории цифровизации судебно-экспертной деятельности рассматриваются цифровые следы и компьютерные средства и системы как носители разыскной и доказательственной криминалистически значимой информации, а также технологии их судебно-экспертного исследования [4, с. 28-29].

Что касается идентификации алгоритмической системы, этот вопрос остается теоретически мало разработанным в отечественной криминалистике. В случаях, когда действия, имеющие правовое значение, совершаются автономными системами на основе ИИ (например, автоматический трейдинг, приведший к ущербу), возникает необходимость идентификации конкретного экземпляра алгоритма, его версии и состояний.

Таким образом, поле идентификации трансформируется от преимущественно материально-фиксированного к информационно поведенческому.

Массовая цифровизация предоставляет в распоряжение субъектов расследования беспрецедентные по своим масштабам и возможностям инструменты:

1. Автоматизированные биометрические системы. Возможности традиционной дактилоскопии и портретной идентификации значительно расширились благодаря внедрению информационных технологий. Автоматизированные системы (например, АДИС «Папиллон» и софт для распознавания лиц) обеспечивают проведение массовых проверок по

обширным базам данных. Их ключевые преимущества — высокая скорость, возможность работы на расстоянии и обработка информации в огромных объёмах, что недостижимо при ручных методах работы эксперта.

2. Анализ больших данных и машинное обучение. Данные технологии открывают доступ к анализу скрытых закономерностей, выявлению аномальных данных и построению поведенческих прогнозов.

3. Цифровая криминалистика. Она предоставляет строгий методический аппарат для изъятия, сохранения и анализа цифровых следов с различных устройств, обеспечивая высокую степень сохранности и документальной фиксации доказательственной информации. Цифровая криминалистика сегодня представляет собой не столько индивидуальную экспертизу, сколько комплекс организационно-технических мер, реализуемых при ключевой, но часто опосредованной роли персонала. Ее фундаментальное отличие от классической криминалистики — в масштабе объекта: от физических носителей и их программного наполнения до цифровых данных, сетевых и облачных артефактов и мобильной инфраструктуры [3, с. 4].

4. Сетевая (ретиальная) идентификация. Сегодня технологии анализа социальных сетей и коммуникационных графов могут помочь идентифицировать участников преступных сообществ, устанавливать роли и иерархию на основе метаданных об их взаимодействиях.

Эти возможности позволяют работать с такими объемами и типами данных, которые ранее были недоступны и могут ускорить процесс расследования.

Наряду с возможностями, цифровизация устанавливает новые пределы для достоверной идентификации и порождает серьезные риски, такие как вероятностный, а не категоричный характер выводов. Алгоритмы машинного обучения и даже сложные биометрические системы (особенно распознавание лиц) работают на основе вероятностных моделей. Их результат – не

утверждение «да/нет», а оценка степени сходства или список вероятных совпадений. Данные результаты подвергаются повторному экспертному исследованию, целью которого является установление тождества объекта самому себе, на основе полученных результатов [5, с. 92].

Также можно выделить проблему «цифрового дуализма» и опосредованности, которая заключается в том, что цифровой след идентифицирует не человека, а его информационное отображение, которое может быть намеренно искажено (фальшивые аккаунты, использование анонимайзеров, VPN, подмена биометрических данных). Установление тождества между цифровым актором и физическим лицом требует дополнительных, зачастую сложных логических построений и привлечения данных из смежных областей. Задача криминалистики – установить связь между событием и лицом, а цифровая среда создает дополнительные промежуточные звенья в этой цепи.

В контексте роста киберпреступности научное сообщество активно пересматривает классические криминалистические категории. Так, исследователь П. В. Мочагин, анализируя формы следообразования в цифровой среде, предлагает адаптировать традиционную двухчастную модель. Он отмечает, что существующее деление на материально-фиксированную и идеальную формы отражения недостаточно для описания преступной деятельности в виртуальном пространстве [6, с. 97]. Ключевым аргументом автора служит принципиальное отличие способа действий: похищение или копирование цифровой информации может быть осуществлено удалённо («виртуальным способом»), без физического присутствия преступника на месте происшествия. Это качественно меняет природу взаимодействия преступника с обстановкой и, как следствие, сам механизм возникновения следов.

Развивая этот подход, В. В. Поляков и С. А. Лапин подчеркивают программно-опосредованную природу электронно-цифровых следов. Ученые

указывают, что их возникновение и любая последующая трансформация всегда являются результатом не прямого, а косвенного воздействия со стороны исполняемого кода компьютерных программ. Эта фундаментальная специфика предопределяет ключевое отличие таких следов от вещественных: они лишены физически воспринимаемых свойств — геометрической формы, цвета, запаха или иных материальных характеристик, привычных для традиционной криминалистики. Следовательно, в цифровых артефактах не могут быть непосредственно запечатлены индивидуальные биометрические или контактные признаки преступника, такие как следы ДНК, папиллярные узоры или запаховые метки, что коренным образом меняет тактику их обнаружения и исследования [7, с. 162—166].

Стоит отметить, что существуют правовые и этические ограничения, при которых массовый сбор и анализ данных для целей идентификации сталкивается с жесткими рамками законодательства о персональных данных (152-ФЗ) и правом на неприкосновенность частной жизни. Можно сделать вывод о том, что использование «сквозной» биометрической идентификации или тотальный анализ цифровых профилей могут быть расценены как непропорциональное вмешательство.

Эффективность процедуры идентификации напрямую обусловлена характеристиками используемого программного обеспечения — его коммерческой версией, конфигурационными настройками и наличием системных уязвимостей. Зависимость от иностранных программных продуктов (ПО) создает системные риски для национальной безопасности и правоприменения. Возможное решение указанной проблемы лежит в плоскости ускоренной разработки и внедрения линейки отечественного программного обеспечения для криминалистических целей. Создание отечественного ПО обеспечит полную прозрачность и контролируемость алгоритмов, что укрепит доверие судов к цифровым доказательствам. Импортозамещение должно включать в себя многочисленные меры и

инициативы со стороны государства: поддержка отечественных производителей и разработчиков программного обеспечения [8, с. 749-752].

Таким образом, в теории криминалистической идентификации еще не нашли отражения такие понятия как «цифровой след» и «цифровой субъект». Следовательно, с развитием современных компьютерных технологий, искусственного интеллекта, рост киберпреступности порождает потребность в расширении науки криминалистики в области идентификации, что будет отражать не только материальные, но и нематериальные-цифровые объекты идентификационного исследования. Отметим, что массовая цифровизация не отменяет классические основы криминалистической идентификации, но радикально усложняет и обогащает ее контекст.

1. Библиографический список

2. Яблоков Н.П. Криминалистика: Учебник / Отв. ред. Н.П. Яблоков. — 3-е изд., перераб. и доп.— М.: Юристъ, 2005. — 781 с. ISBN 5-7975-0728-5 (в пер.)
3. Мещеряков В. А. Основы методики расследования преступлений в сфере компьютерной информации: автореф. дис. .. .д-ра юрид. наук: 12.00.09 / Мещеряков Владимир Алексеевич. — Воронеж, 2001. — 39 с.
4. Мочагин П. В. Новые формы следообразо-ваний в криминалистике и судебной экспертизе // Судебная экспертиза в парадигме российской науки (к 85-летию Ю. Г. Корухова) : сб. материалов 54-х криминалист. чтений. В 2 ч. Ч. 2. — М., 2013.— С. 97—99.
5. Поляков В. В. Средства совершения компьютерных преступлений / В. В. Поляков, С. А. Лапин // Докл. Том. гос. ун-та систем упр. и радиоэлектроники. — Томск, 2014. — С. 162—166.
6. Россинская Е. Р. Учение о цифровизации судебно-экспертной деятельности и проблемы судебно-экспертной дидактики // Правовое государство: теория и практика. 2020. №4 (62). С. 88-101.

7. Саркисян, А. А. Цифровизация судебно-экспертной деятельности : учебное пособие для вузов / А. А. Саркисян. — Москва : Издательство Юрайт, 2025. — 138 с. — (Высшее образование). — ISBN 978-5-534-20447-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 29 — URL: https://urait.ru/bcode/558168/p.29 (дата обращения: 13.12.2025).
8. Слотина Я. А. НЕОБХОДИМОСТЬ ОСУЩЕСТВЛЕНИЯ ИМПОРТОЗАМЕЩЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В СУДЕБНОЙ ЭКСПЕРТИЗЕ // Вестник науки. 2024. №5 (74). С. 749-752.
9. Вехов В.Б. Цифровая криминалистика : учебник для вузов / под редакцией В. Б. Вехова, С. В. Зуева. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 495 с. — (Высшее образование). — ISBN 978-5-534-21152-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/581669 (дата обращения: 13.12.2025).