Научная статья
УДК 343.98
DOI 10.33184/vest-law-bsu-2026.30.18

Купцова Юлия Ильинична
ФГКОУ ВО «Московская академия Следственного комитета Российской Федерации им. А.Я. Сухарева», Москва, Россия, kuptsova.yulia3@yandex.ru

ЦИФРОВОЙ ПРОФИЛЬ КАК ИНСТРУМЕНТ ВЫЯВЛЕНИЯ ПРИЗНАКОВ ПРЕСТУПЛЕНИЯ

Аннотация. В статье рассматривается процесс сбора и хранения цифровых следов в контексте усовершенствования российской правоохранительной и следственной деятельности в рамках профилактики, а также раскрытия и расследования преступлений. Проводя анализ механизма реализации, становится очевидно, что создание таких централизованных систем как ГосСОПКА в совокупности с нормативно-правовой базой «пакета Яровой» обуславливает новый этап развития системы государственного контроля в условиях цифровой трансформации общества, а именно переход от сбора цифровых следов уже совершённого преступления (ретроспективный анализ) к массовому сбору и хранению следов цифровой активности на территории России в режиме реального времени с целью решения прогностической задачи.

Данный подход с применением алгоритмической обработки больших массивов данных сетевой активности ведёт к формированию цифровых профилей граждан, которые впоследствии обрабатываются алгоритмами машинного обучения на основе искусственного интеллекта и разделяются условно на две категории: «нормальная модель поведения» и «модель поведения группы риска». Данный факт с точки зрения законодательства противоречит Конституции Российской Федерации и иным федеральным законам в части гарантий на неприкосновенность частной жизни и защиту персональных данных. Отмечается отсутствие законодательно закреплённого порядка обращения к информации, кому предоставляется право получения информации, содержащейся в цифровых профилях, перечень оснований получения указанной информации для санкции суда.

Ключевые слова: цифровые следы, цифровой профиль, машинное обучение, обработка, частная жизнь, персональные данные, расследование преступления, профилактика.

Для цитирования: Купцова Ю.И. Цифровой профиль как инструмент выявления признаков преступления / Ю.И. Купцова. – 10.33184/vest-law-bsu-2026.30.18 // Вестник Института права Башкирского государственного университета. – 2026. – № 2. – С. 220–228.

Original article

Kuptsova Yulia Ilyinichna
Moscow Academy of the Investigative Committee named after A.Ya. Sukharev, Moscow, Russia, kuptsova.yulia3@yandex.ru.

DIGITAL PROFILE AS A TOOL FOR DETECTING CRIMINAL INVOLVEMENTS

Abstract. The article considers the process of collection and storage of digital traces in the context of Russian law enforcement and investigative activities' improvement within the framework of prevention, as well as detection and investigation of crimes. Analyzing the implementation mechanism, it becomes obvious that the creation of such centralized systems as State detection system of prevention and liquidation of computer attacks consequences (Gossipy), together with the regulatory framework of the Yarovaya package, determines a new stage in the development of the state control system in the context of the digital transformation of society, namely the transition from collecting digital traces of an already committed crime (retrospective analysis) to mass collection and storage of digital activity traces in Russia in real time in order to solve a prognostic problem. This approach, using algorithmic processing of large amounts of network activity data, leads to the formation of digital profiles of citizens, which are subsequently processed by machine learning algorithms based on artificial intelligence and conditionally divided into two categories: "normal behavior model" and "risk group behavior model". From the point of view of legislation, this fact contradicts the Constitution of the Russian Federation and other Federal laws in terms of guarantees for privacy and protection of personal data. It is noted that there is no legislatively enshrined procedure for contacting information who is given the right to obtain information contained in digital profiles, a list of grounds for obtaining this information for court approval.

Key words: digital traces, digital profile, computer-aided learning, processing, privacy, personal data, crime investigation, prevention

For citation: Kuptsova Yu.I. Digital Profile as a Tool for Detecting Criminal Involvements. *Vestnik Instituta prava Bashkirskogo gosudarstvennogo universiteta = Bulletin of the Institute of Law of the Bashkir State University,* 2026, no. 2, pp. 220–228. (In Russian). DOI 10.33184/vest-law-bsu-2026.30.18

Введение. Развитие системы государственного контроля в условиях цифровой трансформации общества сегодня определяется не столько методами изъятия данных с конкретного устройства, сколько технологиями их стратегического накопления из распределённых источников. Этот переход от ретроспективной к прогностической модели, в рамках которой объединяются и хранятся следы цифровой активности на территории России в режиме реального времени, в перспективе будет способствовать изменению подхода правоохранитель-

ных органов не только к расследованию преступлений, но также предупреждению совершения преступных деяний.

Вместе с тем, требуют переосмысления классические криминалистические категории «след» и «доказательство». В России данная тенденция нормативно закреплена через «пакет Яровой»[1], который установил обязательства для операторов сотовой связи по длительному хранению трафика и метаданных. В последующем эта нормативная база реализована и расширена в рамках государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации ГосСОПКА[2] .

Рассмотрение содержания цифрового профиля как индикатора возможной преступной деятельности лица. В контексте предупреждения, пресечения подготавливаемых преступлений традиционное криминалистическое определение цифрового следа как «криминалистически значимой компьютерной информации, т.е. сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи» требует дополнения [1, с. 7]. След перестаёт быть лишь дискретным материальным носителем, привязанным к событию преступления; он становится динамическим элементом потока данных, ценность которого раскрывается лишь в большом массиве собранной и обработанной с использованием алгоритмов машинного обучения информации, при непосредственном сравнении с ранее поступавшими аналогичными по своей природе элементами.

В этой связи приобретает особое значение проблема, на которую обращает внимание А.В. Лисаченко применительно к гражданскому праву. Данная проблема заключается в ретроспективной идентификации, то есть достоверного установления тождества субъекта, совершившего те или иные действия в прошлом [2, с. 96]. Если в гражданско-правовой сфере это касается, например, идентификации лица по архивным данным сделок, то в криминалистической и оперативно-разыскной областях речь идёт о способности алгоритмов машинного обучения спустя месяцы и годы точно связать цифровой след с конкретным лицом, чьи данные хранятся в базах данных операторов связи в рамках «пакета Яровой». Без решения этой ретроспективной задачи даже самая совершенная прогностическая модель рискует оперировать неверно идентифицированными данными, что ставит под сомнение как доказательственное значение результатов, так и законность последующих ограничений прав.

В данной статье под алгоритмами машинного обучения понимается технология, которая не требует программирования каждого шага для поиска решения поставленной задачи. Вместо того, чтобы вручную прописывать алго-

[1] Федеральный закон от 06.07.2016 № 374-ФЗ (ред. от 29.12.2022) «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 29.01.2026).

[2] Концепция, утв. Президентом Российской Федерации 12.12.2014 № К 1274 // Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 08.02.2026).

ритмы для выполнения тех или иных действий, создают универсальные модели, которые «обучаются» на примерах[3].

Таким образом, систематический сбор и анализ таких следов алгоритмами машинного обучения в течение месяцев и лет неизбежно формирует цифровые профили. В рамках настоящего исследования понятие «цифровой профиль» рассматривается в его нормативном правовом значении как совокупность сведений о гражданах и юридических лицах, содержащихся в информационных системах государственных органов, органов местного самоуправления и организаций, осуществляющих в соответствии с федеральными законами отдельные публичные полномочия, а также в единой системе идентификации и аутентификации[4] [3, с. 57, 58]. Это понятие следует сопоставить с иными формами систематизированного учёта данных, такими как Единый федеральный информационный регистр, создаваемый на основании Федерального закона от 08 июня 2020 года № 168-ФЗ «О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации», на основании которого осуществляется сбор широкого спектра сведений о населении, перечисленных в ч. 2 ст. 7 данного Закона.

Правовой предпосылкой этого процесса в России стал «пакет Яровой», законодательно закрепивший массовый сбор и хранение данных операторами сотовой связи в соответствии со ст. 64 Федерального закона от 07 июля 2003 года № 126-ФЗ «О связи». Если изначально его целью был сбор, систематизация и хранение цифровых следов для расследования уже совершённых преступлений, то современные системы, такие как ГосСОПКА, используют эти данные для анализа информации в реальном времени, формируя эмпирическую базу для алгоритмов машинного обучения и выполняя прогностическую задачу. Таким образом, следовая картина выстраивается на основе постоянно пополняемого массива данных, исходя из намерений своевременного выявления, предупреждения и пресечения подготавливаемых преступлений.

Основой данной модели является использование алгоритмов машинного обучения для анализа собранных данных из разрозненных источников. Задача этих алгоритмов состоит в выявлении несоответствий поступивших данных сформированной «эталонной» модели обычного поведения пользователя или группы [4, с. 2]. В последующем алгоритмы машинного обучения при выявлении подобных несоответствий помечают указанный цифровой профиль субъекта как «модель поведения группы риска» и фактически его поведение расценивается системой как подозрительное.

Основаниями подобных решений могут являться случаи, когда граждане используют различные анонимайзеры с целью обхода замедления и блокировки YouTube, для защиты коммерческой тайны, проявляют интерес к политиче-

---

[3] Что такое машинное обучение и как это работает [Электронный ресурс] // URL: https://platformv.sbertech.ru/blog/mashinnoe-obuchenie-machine-learning-chto-eto-i-kak-rabotaet-princzipy-i-zadachi-mashinnogo-obucheniya?utm_referrer=https%3A%2F%2Fya.ru%2F (дата обращения: 08.02.2026).

4 Паспорт проекта ФЗ № 702680-6 // Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 09.02.2026).

ской аналитике, разделяют специфические религиозные или субкультурные практики. Они оцениваются алгоритмами как допустимые, но исходя из статистики являются редкими формами поведения и могут интерпретироваться как «угрожающие» [5, с. 680]. В связи с тем, что цифровой профиль человека является его цифровым двойником, выводы, основанные на работе алгоритмов машинного обучения, распространяются и на личность человека в целом.

Логично предположить, что цифровой профиль, отнесённый к «группе риска», фактически является подозрительным, а значит должен быть подвергнут более детальному анализу и наблюдению за развитием отрицательных тенденций со стороны человека. Таким образом, подозрения должны быть обоснованы не алгоритмами машинного обучения, а человеком, в чью компетенцию входит осуществление контроля за процессом принятия решения, основанного на выводах алгоритма машинного обучения. Необходимо также сосредоточить внимание законодателя на том, что недопустимо принятие решений по ограничению прав и свобод человека только на основании выводов, приведённых алгоритмами машинного обучения. Сегодня, к примеру, алгоритмы машинного обучения на основе искусственного интеллекта могут принять решение по блокировке банковского счёта, если человек сперва снял крупную денежную сумму, а затем пытается её перевести на чужой банковский счёт. Данное решение принял не специалист, который увидел факт подозрительной операции, а машина.

Отнесение цифрового профиля к группе «подозрительных» ведёт к негативным последствиям, таким как автоматический отказ в банковских услугах или трудоустройстве. Выводы делаются на основе скоринга, который анализирует нестандартное поведение и сигнализирует, например, о возможных мошеннических действиях[5]. Подобная дискриминация не имеет законных оснований, не подлежит судебному оспариванию и остаётся для субъекта закрытой процедурой уже долгое время, что ставит под сомнение реализацию права на судебную защиту (ст. 46 Конституции Российской Федерации).

Как справедливо отмечает А.В. Минбалеев, в настоящее время мы наблюдаем так называемый «социальный скоринг», результаты которого для определённой группы граждан будут негативными, так как они не смогут быть «социально дифференцированы как отвечающие тем или иным критериям», что неизбежно приведёт к сегрегации и социальному расслоению общества [6, с. 98].

Рассмотрим подробнее на условном примере совершённого террористического акта, применяя нормы Федерального закона от 06 июля 2016 года № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности». В ходе расследования преступления необ-

[5] Что такое кредитный скоринг и как он работает [Электронный ресурс] // Официальный сайт «СберБанк». URL: https://www.sberbank.ru/ru/person/blog/chto-takoe-skoring-v-banke-prostymi-slovami (дата обращения: 07.02.2026).

ходимо установить факт связи между абонентами как одного из элементов доказывания уже совершённого преступления. В то же время, с целью реализации прогностических задач, алгоритм заранее отмечает эту связь как подозрительную на основании её отклонения от «нормальной модели поведения» или в связи с посещением запрещённых интернет-ресурсов. Таким образом, с точки зрения уголовно-процессуального законодательства, состав преступления отсутствует, но имеются первичные признаки противоправности, которые становятся отклонением от нормы. Это меняет логику в доказывании: не преступление ведёт к поиску следов, а выявленное алгоритмами машинного обучения несоответствие формирует гипотезу о возможном преступлении.

Однако создание цифровых профилей, в контексте реализации прогностических задач, по умолчанию вводит режим тотального негласного наблюдения. Порядок обращения к указанной информации и её использования до настоящего времени законодательно не урегулирован. Это ведёт к нарушению гарантий на неприкосновенность частной жизни, угрожает конституционным правам и свободам человека и гражданина, содержащимся в ст.ст. 22, 23, 24 Конституции Российской Федерации, Федеральном законе от 27 июля 2006 года № 152-ФЗ «О персональных данных»), Федеральном законе от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации». В данном случае человек рассматривается в качестве носителя профиля с определённым коэффициентом риска. Это фактически создаёт категорию «модель поведения группы риска» для лиц, чьи цифровые привычки алгоритм помечает как не соответствующие «нормальной» модели, даже при полном отсутствии события преступления [7, с. 11, 12].

Одновременно с этим, концентрация детализированных цифровых профилей создаёт мощный соблазн использовать их вне заявленных целей борьбы с киберпреступлениями и тяжкими преступлениями, например, для политического контроля, давления на оппозицию, бизнес-разведки или сбора компромата [8, с. 95].

В рамках изучения вопроса сбора информации и тотального контроля, стоит отметить, что с 2017 года ПАО «Мегафон» запустила и успешно ведёт проект «Мегафон-Таргет», который даёт корпорациям и компаниям возможность привлекать новых клиентов с помощью таких каналов продвижения как баннеры в интернете, рассылки sms, mms, e-mail и другие. Они используют более 100 параметров для формирования и обновления целевой аудитории. Основными из них являются: социально-демографические (пол, возраст, дата рождения, семейное положение, наличие или отсутствие детей), геопозиция, сферы интересов и другие[6]. Сбор данных осуществляется с применением технологии глубокого обучения на основе сбора и систематизации данных об активности группы абонентов, объединённых только признаками. Пользователь,

[6] Точно в цель: как технологии изменили инструменты таргетирования рекламы [Электронный ресурс] // Официальный сайт «РБК». URL: https://trends.rbc.ru/trends/industry/cmrm/64e5a6bd9a7947d62390563e (дата обращения: 05.02.2026).

подключивший данную услугу, при запуске рассылки по базе оператора может видеть только количество отправленных сообщений и количество людей, перешедших по ссылке. Персональные данные остаются для него скрыты, однако ими обладает компания, предоставляющая эту услугу. Стоит отметить, что 31 марта 2025 года стало известно об утечке персональных данных абонентов ПАО «МегаФон», которую оператор впоследствии опроверг.

В России отсутствуют действенные механизмы судебного санкционирования запросов к таким массивам, а требования ст. 9 Федерального закона от 12 августа 1995 года № 144-ФЗ «Об оперативно-розыскной деятельности», где указано, что «основанием для решения судьёй вопроса о проведении оперативно-розыскного мероприятия, ограничивающего конституционные права граждан, указанные в части первой настоящей статьи, является мотивированное постановление одного из руководителей органа, осуществляющего оперативно-розыскную деятельность», носят формальный характер. Что должно в нём содержаться? Какая объективная мотивация, если это вывод алгоритмов машинного обучения, который не имеет юридической силы и может быть ложным? Каким образом получить судебную санкцию на проведение ОРМ в отношении информации, собираемой и анализируемой для выполнения прогностических задач?

С учётом выявленных угроз и неопределённостей, необходимо детально, на законодательном уровне разрешить вопрос разработки перечня предоставляемых сведений, основания и порядок ознакомления с ними, какой орган и согласно какому алгоритму действий сможет получать доступ к интересующей информации. Данный подход может способствовать противодействию выявляемым угрозам. Видится необходимым закрепление разделённого режима доступа к таким данным, не связанным с конкретным расследуемым делом, который должен требовать судебного санкционирования, обоснованием которого будет являться указание конкретных параметров поиска и анализа.

В этой связи, необходимо законодательно установить чёткие и максимально короткие сроки автоматического уничтожения данных, не востребованных в рамках возбуждённых уголовных дел, за исключением информации, относящейся к расследуемым преступлениям из ограниченного перечня тяжких и особо тяжких составов.

С целью минимизации риска умышленной дискриминации, необходимо создать контролирующий орган, непосредственной задачей которого будет являться проверка алгоритмов аналитических систем на предмет предвзятости и соответствия заявленным, а не скрытым целям.

С целью повышения уровня доверия к рассматриваемой модели, отвечающей прогностическим задачам, и систем на её основе, лицо, в отношении которого алгоритмами машинного обучения принято решение об отказе в услуге, о включении в группу риска и другие, должно иметь право на получение уведомления с мотивированными разъяснениями данного решения и в объёме, не наносящем ущерб государству, корпорации и уголовно-правовой системе

(в рамках расследования конкретного уголовного дела), а также возможность его судебного оспаривания.

Заключение. Подводя итог вышеизложенному, можно утверждать, что при выполнении прогностической задачи сбор, анализ и систематизация цифровых следов перестали быть техническим вопросом и превратились в центральный фактор, определяющий уровень государственного контроля в условиях цифровой трансформации общества. Прогностическая задача, реализуемая в современных государственных системах, потенциально повышает эффективность противодействия угрозам безопасности государства и общества, однако следствием подобного повышения эффективности становится изменение подхода к рассмотрению принципов уголовного процесса и правового статуса личности. Без введения ограничений на законодательном уровне, основанных на судебном контроле, прозрачности процедуры и гарантиях против дискриминации, государственная система контроля рискует создать общество, где цифровая тень человека будет постоянно опережать и менять его судьбу, нарушая его конституционные права.

Список источников

1. Багмет А.М., Бычков В.В., Ильин Н.Н., Скобелин С.Ю. Цифровые следы преступлений: монография / А.М. Багмет, В.В. Бычков, Н.Н. Ильин, С.Ю. Скобелин – Москва : Проспект, 2021. – 168 с.

2. Лисаченко А.В. Идентификация субъектов гражданских правоотношений: новые проблемы и некоторые решения / А.В. Лисаченко // Российский юридический журнал. – 2019. – № 5. – С. 91–99.

3. Жарова А.К. Вопросы обеспечения безопасности цифрового профиля человека / А.К. Жарова // Юрист. – 2020. – № 3. – С. 55–61.

4. Szymielewicz K. The layers of your online profile / K. Szymielewicz // Panoptykon Foundation. – 2019 [Электронный ресурс]. – URL: https://en.panoptykon.org/articles/three-layers-your-digital-profile (дата обращения: 07.02.2026).

5. Barocas S., Selbst A.D. Big Data's Disparate Impact / S. Barocas, A.D. Selbst // California Law Review. – 2016. – Vol. 104, № 3. – P. 671–732.

6. Минбалеев А.В. Проблемы социальной эффективности и защиты прав человека при использовании искусственного интеллекта в рамках социального скоринга / А.В. Минбалеев // Вестник Южно-Уральского государственного университета. Серия: Право. – 2020. – Т. 20. – № 2. – С. 96–101.

7. Ревякин С.А. Влияние процессов цифровизации на права человека и развитие гражданского общества / С.А. Ревякин // Информационно-аналитический бюллетень о развитии гражданского общества и некоммерческого сектора в России. – 2021. – № 2(21). С. 6–13.

8. Напсо М.Д., Напсо М.Б. Тренды цифровой трансформации общества: актуальные проблемы реализации прав индивида в сфере информации / М.Д. Напсо, М.Б. Напсо // Журнал российского права. – 2021. – № 10. – С. 85–97.

References

1. Bagmet A.M., Bychkov V.V., Ilyin N.N., Skobelin S.Yu. Digital Crimes' Traces: Monograph. Moscow, Prospect, 2021. 168 p. (In Russia).

2. Lisachenko A.V. Identification of Subjects of Civil Legal Relations: New Problems and Some Solutions. *Russian Juridical Journal*, 2019, no. 5, pp. 91–99. (In Russia).

3. Zharova A.K. Issues of Ensuring Security of a Person's Digital Profile. *Jurist,* 2020, no. 3, pp. 55–61. (In Russia).

4. Szymielewicz K. The Layers of Your Online Profile. Panoptykon Foundation, 2019. URL: https://en.panoptykon.org/articles/three-layers-your-digital-profile (In English).

5. Barocas S., Selbst A.D. Big Data's Disparate Impact. *California Law Review*, 2016, vol. 104, no. 3, pp. 671–732. (In English).

6. Minbaleev A.V. Problems of Social Efficiency and Human Rights Protection in the Use of Artificial Intelligence in the Framework of Social Scoring. *Bulletin of South Ural State University. Series: Law*, 2020, vol. 20, no 2, pp. 96–101. (In Russia).

7. Revyakin S.A. The Impact of Digitalization on Human Rights and Civil Society Development. *Information and Analytical Bulletin on the Development of Civil Society and the Non-Profit Sector in Russia*, 2021, no. 2(21), pp. 6–13. (In Russia).

8. Napso M.D., Napso M.B. Digital Transformation Trends in a Society: Actual Problems Arising in Realization of the Rights of the Individual in Information Sphere. *Journal of Russian Law,* 2021, no. 4, pp. 89–97. (In Russia).

Информация об авторе

Купцова Юлия Ильинична – *младший научный сотрудник*

Information about the Author

Kuptsova Yulia Ilyinichna – *Junior Research Fellow*

Статья поступила в редакцию 19.02.2026 г.; одобрена после рецензирования 12.06.2026 г.; принята к публикации 13.06.2026 г.

The article was submitted 19.02.2026; approved after reviewing 12.06.2026; accepted for publication13.06.2026.