

**Бессонова Марина Николаевна**

магистрант

*Научный руководитель*

**Фастова Марина Андреевна**

канд. юрид. наук, доцент

ФГБОУ ВО «Российский государственный

социальный университет»

г. Москва

## ЦИФРОВОЙ СЛЕД КАК ПЕРСОНАЛЬНЫЕ ДАННЫЕ: ПРОБЛЕМЫ ДЕЛИМИТАЦИИ И ОХРАНЫ В ПОВЕДЕНЧЕСКОЙ РЕКЛАМЕ

**Аннотация:** статья посвящена комплексному анализу проблематики делимитации цифрового следа и персональных данных в контексте правового регулирования поведенческой (таргетированной) рекламы. На основе анализа Федерального закона №152-ФЗ «О персональных данных» выявлена недостаточная адаптивность правового регулирования к специфике цифровых следов (cookie-файлы, IP-адреса, история поисковых запросов, поведенческие паттерны). Проанализированы коллизии между режимом персональных данных и обезличенной информации, механизмы получения согласия на обработку данных в целях таргетированной рекламы. Проведено сопоставление российского и европейского (GDPR) подходов, выявлены пробелы в законодательстве. Сформулированы предложения по совершенствованию правовых механизмов: разработка законодательного определения цифрового следа, уточнение критериев идентифицируемости информации, введение института «цифрового согласия».

**Ключевые слова:** делимитационный анализ, идентификационная детерминанта, киберправовая догматика, поведенческий таргетинг, презумпция обезличенности, протективный режим, цифровая экзистенция.

Эпоха постиндустриального общества характеризуется фундаментальной трансформацией способов производства, обработки и коммерциализации информации. В этих условиях каждый акт взаимодействия субъекта с информационно-телекоммуникационной сетью «Интернет» порождает комплекс следовых данных, фиксирующих параметры его информационного поведения. Совокупность таких следов образует многослойную структуру, получившую в научной литературе наименование «цифровой след» (digital footprint) – термин, заимствованный из англоязычной правовой доктрины, однако до сих пор не нашедший закрепления в российском законодательстве.

Проблематика правового статуса цифрового следа приобретает особую актуальность в контексте правового регулирования поведенческой рекламы – технологии демонстрации рекламных сообщений, основанной на анализе предпочтений, интересов и поведенческих паттернов конкретного пользователя. В отличие от традиционной массовой рекламы, ориентированной на абстрактного потребителя, поведенческий таргетинг оперирует персонифицированными данными, что неизбежно ставит вопрос о соответствии таких практик требованиям законодательства о персональных данных.

### *1. Теоретические основания понятия «цифровой след» в правовом дискурсе.*

#### *1.1. Содержательная характеристика феномена цифровой экзистенции.*

Цифровой след представляет собой совокупность следовых данных, генерируемых в результате активности субъекта в цифровой среде. Данный феномен носит двойственный характер: с одной стороны, он фиксирует объективные параметры взаимодействия пользователя с техническими средствами (время доступа, IP-адрес, геолокационные координаты, тип устройства); с другой – отражает субъективные характеристики его информационного поведения (поисковые запросы, история просмотров, кликовая активность, временные паттерны потребления контента).

В отечественной доктрине информационного права выделяют два типа цифровых следов: активные (порождаемые целенаправленными действиями субъекта – публикациями в социальных сетях, комментариями, заполнением веб-

форм) и пассивные (формируемые автоматически без прямого намерения пользователя – технические логи, cookie-файлы, метаданные). Именно пассивные следы вызывают наибольшие правовые затруднения, поскольку их сбор осуществляется скрытно, а субъект часто не осознаёт факт и объём фиксируемой информации.

Правовая природа цифрового следа остаётся дискуссионной. Часть исследователей отождествляет его с персональными данными, основываясь на потенциальной идентифицируемости информации. Другие настаивают на автономности данного института, указывая на специфику его генезиса, структуры и режима оборота.

### *1.2. Идентификационная детерминанта как критерий правовой квалификации.*

Ключевым критерием для отнесения цифрового следа к категории персональных данных выступает идентификационная детерминанта – способность информации прямо или косвенно определять личность субъекта. Согласно статье 3 Федерального закона № 152-ФЗ, персональные данные – это любая информация, относящаяся к прямо или косвенно определённом или определяемому физическому лицу (субъекту персональных данных).

Однако применительно к цифровым следам данное определение демонстрирует свою неопределённость. Так, IP-адрес в изолированном виде не позволяет идентифицировать конкретное лицо, однако в совокупности с данными интернет-провайдера он становится мощным идентификатором. Аналогичная ситуация складывается с cookie-файлами: сами по себе они представляют набор символов, не содержащих прямых персональных сведений, однако в сопряжении с профильными данными пользователя формируют детальный цифровой портрет.

В доктрине информационного права сформировался подход, согласно которому правовая квалификация цифрового следа должна осуществляться с учётом контекста его обработки, технических возможностей идентификации и целей использования. Данный контекстуальный подход находит отражение в позиции Европейского суда по правам человека, который в ряде решений признал, что даже

обезличенные данные могут приобретать статус персональных при наличии соответствующих технических средств их реидентификации.

## *2. Правовое регулирование поведенческой рекламы в российском законодательстве.*

### *2.1. Коллизии между режимом персональных данных и режимом обезличенной информации.*

Поведенческая реклама функционирует на основе алгоритмического анализа цифровых следов пользователей с целью прогнозирования их потребительских предпочтений и демонстрации релевантных рекламных сообщений. Технологическая основа данного процесса – programmatic-платформы, осуществляющие автоматизированную покупку рекламного инвентаря в режиме реального времени.

В российском правовом поле поведенческий таргетинг регулируется фрагментарно. Федеральный закон от 13.03.2006 № 38-ФЗ «О рекламе» не содержит специальных норм, посвящённых таргетированной рекламе, ограничиваясь общими положениями о недопустимости использования персональных данных без согласия гражданина. В свою очередь, Федеральный закон № 152-ФЗ устанавливает обязанность оператора получать согласие субъекта на обработку его персональных данных, однако механизм такого согласия в контексте цифровых следов остаётся недостаточно проработанным.

Существенной проблемой выступает презумпция обезличенности – допущение о том, что данные, прошедшие процедуру обезличивания, утрачивают статус персональных и могут свободно обрабатываться. На практике технологии реидентификации (деанонимизации) позволяют восстановить привязку обезличенных наборов данных к конкретным субъектам, что делает презумпцию обезличенности юридически несостоятельной в условиях современных big data-технологий.

### *2.2. Институт согласия в контексте цифровых следов.*

Согласие субъекта персональных данных представляет собой волеизъявление, посредством которого физическое лицо разрешает обработку своих персональных данных. В традиционном понимании согласие должно быть конкретным, информированным и добровольным. Однако в сфере поведенческой рекламы эти требования систематически нарушаются.

Практика использования так называемых «cookie-баннеров» (всплывающих уведомлений о сборе cookie-файлов) демонстрирует формализм подхода к получению согласия. Пользователь, нажимая кнопку «Принять», зачастую не получает исчерпывающей информации о характере, объёме и целях обработки его цифровых следов, а равно о субъектах, которым будут переданы данные. Такое согласие носит фиктивный характер и не отвечает требованиям статьи 9 Федерального закона № 152-ФЗ.

В перспективе следует закрепить такое определение, как «цифровое согласие» – специфическую разновидность согласия субъекта, учитывающую специфику цифровых следов. Данное согласие должно включать: многоуровневую структуру согласия, разграничивающую сбор технических метаданных и поведенческих паттернов; динамичность согласия, допускающую его отзыв в любой момент без необоснованных ограничений; прозрачность алгоритмов обработки, обеспечивающую понимание субъектом механизмов формирования рекламных предложений.

### *3. Сравнительно-правовой анализ режимов охраны цифрового следа.*

#### *3.1. Европейская модель: GDPR и директива ePrivacy.*

Общеевропейский подход к регулированию обработки цифровых следов базируется на положениях Регламента ЕС 2016/679 (General Data Protection Regulation, GDPR). GDPR устанавливает расширенное толкование понятия персональных данных, включающее любую информацию, относящуюся к идентифицированному или идентифицируемому физическому лицу, при этом идентифицируемость определяется с учётом всех средств, которые могут быть использованы оператором или третьими лицами.

Особое значение для регулирования поведенческой рекламы имеет Директива 2002/58/ЕС (Директива о конфиденциальности и электронных коммуникациях), предусматривающая запрет на использование cookie-файлов и иных средств отслеживания без информированного согласия пользователя.

Сравнительный анализ выявляет принципиальные различия между российским и европейским подходами. GDPR опирается на презумпцию защищённости данных и требует наличия правовых оснований для любой операции обработки. Российское законодательство, напротив, исходит из презумпции свободы обработки обезличенной информации, что создаёт благоприятные условия для непрозрачных практик сбора цифровых следов.

### *3.2. Пробелы в российском законодательстве и направления их устранения.*

Анализ действующего законодательства позволяет выделить ряд критических пробелов, снижающих эффективность охраны цифрового следа в контексте поведенческой рекламы.

Во-первых, отсутствие законодательного определения цифрового следа приводит к неопределённости правовых границ данного феномена. В научной литературе предлагаются различные интерпретации, однако ни одна из них не получила нормативного закрепления.

Во-вторых, механизм обезличивания персональных данных, предусмотренный статьёй 13.1 Федерального закона № 152-ФЗ, не содержит технических критериев, позволяющих гарантировать необратимость утраты идентифицируемости. Это открывает возможности для легитимации де-факто персонализированной обработки данных под видом работы с обезличенными массивами.

В-третьих, институт согласия не адаптирован к специфике автоматизированной обработки цифровых следов в реальном времени. Традиционная модель «разрешить/запретить» не учитывает сложность современных экосистем данных, где информация передаётся множеству субъектов и подвергается многоуровневой обработке.

## *4. Механизмы совершенствования правовой охраны цифрового следа.*

### *4.1. Протективный режим цифровой экзистенции.*

На основании проведённого анализа представляется целесообразным предложить формирование протективного режима (защитного режима) цифровой экзистенции – совокупности правовых гарантий, обеспечивающих субъекту контроль над его цифровыми следами и ограничивающих возможности их несанкционированного использования в коммерческих целях.

Первоочередной мерой выступает введение в законодательство специализированного определения цифрового следа, фиксирующего его структурные элементы (активные и пассивные компоненты), способы генезиса и критерии отграничения от персональных данных и иных категорий информации.

Вторым направлением является уточнение критериев идентифицируемости информации. Предлагается закрепить презумпцию персональности цифровых следов, порождаемых в результате длительного наблюдения за пользователем (продолжительностью более установленного законом порога), независимо от наличия прямых идентификаторов.

Третье направление связано с институционализацией «цифрового согласия», предусматривающего обязанность оператора предоставлять пользователю исчерпывающую информацию о логике алгоритмов формирования поведенческого профиля, субъектах, получающих доступ к данным, и сроках их хранения.

### ***Список литературы***

1. Белл Д. Грядущее постиндустриальное общество / Д. Белл. – М., 1999. – С. 15.
2. Бачило И.Л. Информационное право: учебник для вузов / И.Л. Бачило. – М.: Юрайт, 2023. – С. 89.
3. Акашев Ю.И. Правовое регулирование рекламной деятельности / Ю.И. Акашев, Г.Д. Кулагин // Молодой ученый. – 2022.
4. Федеральный закон «О персональных данных» №152-ФЗ от 27.07.2006.
5. Ковалева Н.Н. Информационное право: учебник для вузов / под ред. Н.Н. Ковалевой. – М.: Юрайт, 2025. – 353 с.

6. Миненбаев Г.Ф. Основные проблемы и вызовы применения цифровых следов / Г.Ф. Миненбаев // Международный журнал гуманитарных и естественных наук. – 2025.
7. Гадельшин А.А. Cookie-файлы как объект персональных данных и способ нарушения конфиденциальности персональных данных / А.А. Гадельшин, М.М. Степанов // Вопросы российской юстиции. – 2021.
8. Приказ Роскомнадзора от 19 июня 2025 года №140 устанавливает требования к обезличиванию персональных данных и методы их обработки.
9. Ohm P. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization / P. Ohm // UCLA Law Review. – 2010. – Vol. 57. – P. 1723.
10. Как файлы cookies влияют на кибербезопасность // Редакция Falcongaze. – 2025.
11. Постановление ЕСПЧ по делу «S. and Marper v. the United Kingdom» от 04.12.2008 (жалобы №30562/04 и 30566/04).
12. Щепилова Г.Г. Маркетинговое и правовое обеспечение рекламной деятельности / Г.Г. Щепилова. – М.: Юрайт, 2018. – С. 381. EDN QPBWGC
13. Zuboff S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power / S. Zuboff. – New York: PublicAffairs, 2019.
14. Федеральный закон «О рекламе» №38-ФЗ от 13.03.2006. – Ст. 10.
15. Постановление Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» №1119 от 01.11.2012. – П. 2.
16. Регламент ЕС 2016/679 (GDPR). – Преамбула (42).
17. Регламент ЕС 2016/679 (GDPR). – Ст. 26, 30, 32, 33.
18. Регламент ЕС 2016/679 от 27.04.2016. – Ст. 23, 24, 26.
19. Директива 2002/58/ЕС от 12.07.2002. – Ст. 25.
20. Регламент ЕС 2016/679. – Ст. 42.
21. Минцифры предлагает собирать персональные данные россиян за счет бизнеса // Журнал Форбс. – 2023.



22. Бондаренко Н.Л. Правовая и организационная природа процессов цифровизации и регуляторная функция государства в данной сфере / Н.Л. Бондаренко, Ю.Г. Конаневич // *Ex Jure*. – 2021. – №1. – С. 56–67. DOI 10.17072/2619-0648-2021-1-56-67. EDN OZFAFE

23. Бондаренко Н.Л. Дискуссия о системе права и ее значение для цивилистической науки / Н.Л. Бондаренко, Ю.Г. Конаневич, О. Шкут // *Методологические проблемы цивилистических исследований*. – 2022. – №4. – С. 11–28. DOI 10.33397/2619-0559-2022-4-4-11-28. EDN WVAKDT

24. Бондаренко Н.Л. Юридическая квалиметрия как новая отрасль правового научного знания / Н.Л. Бондаренко, Ю.Г. Конаневич // *Право.by*. – 2022. – №5. – С. 117–124. EDN KCSRAO

25. Бондаренко Н.Л. Фискальное регулирование и фискальное право: проблемы идентификации и институционализации / Н.Л. Бондаренко, Ю.Г. Конаневич, Е.Н. Гладкая // *Право.by*. – 2022. – №1. – С. 46–51. EDN OGDKWH

26. Липунов В.И. Искусственный интеллект и тренды цифровизации: техногенный прорыв как вызов праву / В.И. Липунов // *Искусственный интеллект и тренды цифровизации: техногенный прорыв как вызов праву: материалы Третьего Международного транспортно-правового форума (Москва, 10–11 февраля 2021 г.)*. – М.: Российский университет транспорта, 2021. – С. 241–249. EDN PBDDMP