Научная статья
УДК 343.2/.7
DOI: 10.47475/2311-696X-2026-50-3-96-101
С. 96–101

БОЛЬШИЕ ДАННЫЕ (BIG DATA) В СОЦИАЛЬНОМ ГОСУДАРСТВЕ: НОВЫЕ ОБЪЕКТЫ УГОЛОВНО-ПРАВОВОЙ ОХРАНЫ

Алексей Александрович Ходусов

Международный юридический институт, Москва, Россия
yustas-73@mail.ru
https://orcid.org/0000-0001-6968-0989

Аннотация. В данной статье проблема определяется современной ситуацией с правовым регулированием больших данных (Big Data) в российском праве, выявлением основных пробелов и коллизий законодательства в этой сфере. Выявить возможности применения Big Data для защиты социальных прав граждан, а также перспективы их использования в различных сферах законодательства — от налогового до трудового права. Юридическим методом определяются обстоятельства, по которым Big Data следует рассматривать в качестве новых объектов уголовно-правовой охраны, учитывая их высокую общественную опасность при незаконном обороте.

Методом анализа правовой неопределенности и пробелов в законодательстве определяются угрозы правам граждан в социальном государстве, включая риск дискриминации, утечки персональных данных и цифрового контроля. Методом сбора информации осуществляется выявление, каким образом осуществляется раскрытие преступлений, в том числе в рамках оперативно-розыскной деятельности.

Охарактеризованы основные пробелы и коллизии законодательства в сфере правового регулирования больших данных (Big Data); определен функционал больших массивов данных (Big Data) который открывает новые возможности для правового регулирования больших данных (Big Data) в российском праве.

Ключевые слова: большие данные (Big Data), компьютерная информация, персональные данные, уголовно-правовая охрана, преступления, права граждан

Для цитирования: Ходусов А. А. Большие данные (Big Data) в социальном государстве: новые объекты уголовно-правовой охраны // Правопорядок: история, теория, практика. 2026. № 3 (50). С. 96–101. DOI: 10.47475/2311-696X-2026-50-3-96-101

Research article

BIG DATA IN THE SOCIAL STATE: NEW OBJECTS OF CRIMINAL LAW PROTECTION

Aleksey A. Khodusov

International Law Institute, Moscow, Russia
yustas-73@mail.ru
https://orcid.org/0000-0001-6968-0989

Abstract. This article examines the current legal regulation of Big Data in Russian law, identifying key gaps and conflicts of law in this area. It explores the potential for Big Data to protect citizens' social rights, as well as the prospects for its use in various areas of legislation, from tax law to labor law. Using a legal approach, it identifies the circumstances under which Big Data should be considered new objects of criminal law protection, given its high social danger when illicitly traded.

By analyzing legal uncertainty and gaps in legislation, it identifies threats to citizens' rights in a welfare state, including the risk of discrimination, personal data leakage, and digital surveillance. Information collection is used to identify methods for solving crimes, including through investigative operations.

The article characterizes the key gaps and conflicts of law in the area of Big Data regulation, and identifies the functionality of Big Data that opens up new opportunities for the legal regulation of Big Data in Russian law.

Keywords: Big Data, computer information, personal data, criminal law enforcement, crime, civil rights

© Ходусов А. А.

For citation: Khodusov A. A. Big Data in the social state: new objects of criminal law protection. *Pravoporyadok: istoriya, teoriya, praktika* [Legal and Order: History, Theory, Practice]. 2026;(3):96-101. (In Russ.). DOI: 10.47475/2311-696X-2026-50-3-96-101

Введение

В российском законодательстве большие данные (Big Data), как отдельный объект уголовно-правовой охраны, не выделяются. Правовое регулирование в этой сфере строится через призму других категорий, в частности, персональных данных и компьютерной информации.

Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Они могут содержаться как в памяти ЭВМ или других компьютерных устройств, так и на любых внешних электронных носителях.

Персональные данные — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). К ним относятся, например, ФИО, дата рождения, ИНН, адрес, телефон, семейное положение, социальное положение, имущественное положение, образование, профессия, занимаемая должность, стаж работы, доходы и иная информация.

Правовое регулирование больших данных

С юридической точки зрения большие данные рассматриваются, как технологии сбора, обработки и хранения информации, характеризующиеся большим объемом, скоростью, разнообразием и изменчивостью данных [1, с. 49–52]. Если в состав таких данных входят персональные данные, к ним применяются нормы Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

В Гражданском кодексе РФ наиболее близкой категорией к большим данным являются базы данных, но их правовое понимание (совокупность самостоятельных материалов, например статей, расчетов) не совпадает с концепцией больших данных.

С 11 декабря 2024 года в Уголовном кодексе РФ действует статья 272.1 «Незаконные использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения». Она введена Федеральным законом от 30 ноября 2024 г. № 421-ФЗ.

Ключевое условие наступления ответственности по ст. 272.1 УК РФ — одновременное наличие двух составляющих в действиях виновного лица:

— незаконный способ завладения персональными данными в электронном виде.

— незаконные действия, связанные с их распространением, использованием, сбором или хранением.

Таким образом, хотя большие данные, как таковые, не являются самостоятельным объектом уголовно-правовой охраны, их обработка может подпадать под действие ст. 272.1 УК РФ, если в них содержатся персональные данные и совершены указанные в статье противоправные действия [2, с. 40].

До сих пор правовой статус данных, используемых этими инструментами, неоднороден [3, с. 1–5]. Законодательство различает персональные данные, позволяющие идентифицировать человека; обезличенные данные, которые невозможно отнести к конкретному лицу; и, наконец, большие данные (Big Data) — огромные и сложные совокупности информации, обработка которых требует специальных технологий. Правовой режим Big Data, как единого целого в российской юриспруденции, только формируется. Это то, что и создает дополнительные сложности для его применения [4, с. 34].

Big Data представляют собой новые объекты уголовно-правовой охраны по следующим обстоятельствам.

Во-первых, функционал Big Data обуславливает и потенциал для профилактики преступлений против социальных прав уже сегодня меняет подходы правоохранительных и контролирующих органов. Наиболее ярким примером является борьба с мошенничеством в сфере социальных выплат.

Алгоритмы машинного обучения, анализируя огромные массивы данных из различных государственных реестров (налоговых, пенсионных, регистрационных), способны выявлять сложные аномалии и корреляции, невидимые для человека. Так, проиллюстрировать сказанное можно следующим примером: автоматизированная система выявляет ситуации, при которых начисление выплат продолжается на счет уже умершего получателя. К той же категории относятся случаи параллельного незаконного получения пособий одним лицом в нескольких субъектах Федерации одновременно [5, с. 41–45].

Во-вторых — и здесь уместно оговориться — применяемые технологии формируют существенный задел для усиления гарантий социальных прав. Аналитические системы, построенные на технологиях Big Data, обладают прогностическим потенциалом: они способны заблаговременно распознавать мошеннические схемы, фиксировать системные нарушения, обнаруживать иные противоправные деяния. Вместе с тем обращает на себя внимание и обратная сторона процесса. Большие данные сами превращаются в источник принципиально новых форм преступных посягательств. [6, с. 223–228]. Среди них — так называемая «алгоритмическая дискриминация», целенаправленное манипулятивное воздействие на социально уязвимые категории граждан, наконец, масштабные посягательства на конфиденциальность персональной информации [9,

© Ходусов А. А.

с. 292–301]. Возникает правовой вакуум, когда традиционные нормы уголовного закона оказываются недостаточно приспособленными для квалификации новых общественно опасных деяний. Часто правоприменитель сталкивается с проблемами установления вины и субъекта преступления в условиях работы «автономных» алгоритмов.

В-третьих, проблема заключается в фундаментальном противоречии между экспоненциальным развитием технологий больших данных и явным отставанием в развитии уголовно-правовых средств [8, с. 800–804].

Уголовно-правовые средства предназначены для выполнения двух ключевых функций: 1) защиты социальных прав от новых «цифровых» посягательств, и 2) регулирования криминогенных рисков, порождаемых самими этими технологиями. Но существующее уголовное законодательство (в его текущей редакции) зачастую в полной мере не может охватить специфику общественно опасных деяний, совершаемых с использованием цифровых алгоритмов.

Применение Big Data несет с собой немало возможностей, но вместе с тем поднимает серьезные вопросы и угрозы, особенно в сфере социальных прав.

К основным рискам, связанным с тем, как собираются, обрабатываются и используются данные о людях без их полного понимания или согласия, можно отнести следующие.

1. Право на приватность под угрозой. Технологии Big Data открывают возможность аккумулировать колоссальные объёмы сведений о конкретном человеке — здесь и геолокация, и поведенческие привычки, и круг социальных контактов, и даже данные медицинского характера.

2. Социальная предвзятость, оборачивающаяся дискриминацией. Алгоритмические системы, чье обучение опирается на исторические данные, нередко воспроизводят уже сложившиеся стереотипы, а в отдельных случаях — и усиливают их.

3. Утрата контроля над персональными сведениями. Нередко человек попросту не осведомлён о том, какая именно информация о нём собирается — равно как не знает он ни о субъектах этого сбора, ни о преследуемых ими целях.

4. Воздействие на свободу выбора и формирование мнения. Благодаря технологиям Big Data возникают «фильтрующие пузыри» — ситуации, при которых индивид сталкивается исключительно с теми сведениями, что согласуются с его предшествующим поведением.

5. Угрозы для уязвимых групп — люди с низким доходом — чаще всего страдают от автоматизированных систем оценки.

Новые угрозы социальным правам, связанным с применением Big Data предложение 1 (табл. 1).

Анализ угроз социальным правам, связанных с Big Data, показывает системную пробельность современного уголовного законодательства.

Для выявления роли больших данных в защите прав граждан в социальном государстве выделим основания для определения организационно-правовых форм характеризуемой защиты, к которым, по нашему мнению, следует отнести технологии применения Big Data; возможности их использования для различных сфер законодательства и для анализа судебной практики [7, с. 387–420].

Действительно, большие данные играют двойственную, но очень важную роль в защите прав граждан в социальном государстве — они могут как способствовать защите, так и создавать новые риски.

С одной стороны, большие данные позволяют государству более эффективно реализовывать социальные программы. Например, анализируя объемные массивы информации о доходах, занятости, здоровье и образовании, власти могут точнее выявлять нуждающихся, оперативно назначать пособия и контролировать, чтобы помощь дошла до тех, кому она действительно необходима. Это делает социальную политику более справедливой и персонализированной.

Кроме того, с помощью анализа больших данных можно выявлять дискриминацию, нарушения трудовых прав или неравный доступ к медицине и образованию. Например, если в определенном регионе системно отказывают в льготах людям с инвалидностью — такие паттерны хорошо «ловятся» алгоритмами.

Однако, с другой стороны, сбор и использование больших данных (Big Data) несет серьезные риски для прав граждан. Когда информация о человеке собирается из множества источников — от банков и соцсетей до камер и медицинских карт — формируется его «цифровой профиль», который может использоваться без его ведома или согласия. Это угрожает праву на неприкосновен-

Таблица 1 — Новые угрозы социальным правам, связанные с Big Data

Угроза	Сущность нарушения	Проблема квалификации
Цифровая дискриминация	Автоматизированный, алгоритмический отказ в предоставлении услуг определенным социальным группам.	Сложность доказывания умысла и субъекта преступления (кто виноват: разработчик, владелец или пользователь?).
Манипулятивное воздействие	Таргетированное распространение дезинформации с целью лишить человека социальных прав или льгот.	Состав мошенничества часто требует дополнения для учета специфики цифрового манипулирования.
Алгоритмическая несправедливость	Автоматическое принятие несправедливых решений в соцсфере из-за «заточенных» под определенный результат алгоритмов.	Пробелы в законодательстве: отсутствие нормы, прямо криминализирующей последствия использования недобросовестных алгоритмов.

© Ходусов А. А.

ность частной жизни, на свободу от слежки и на защиту персональных данных.

Особенный риск состоит в том, что когда решения о человеке — например, в кредите, трудоустройстве или социальной поддержке — принимаются автоматически, на основе алгоритмического скоринга. Данная система может вести к цифровой дискриминации: человеку отказывают не по заслугам или вине, а потому что он отнесен к категории ненадежности.

В данном случае, ключевое — не просто использовать большие данные (Big Data), а делать это прозрачно, этично и с уважением к правам. Гражданин должен понимать, какие данные о нем собираются, зачем и как они используются. Он должен иметь право на доступ, исправление и удаление своих данных, а также на возражение против автоматизированных решений.

Следует отметить, что в России, уже есть конституционное основание для этого: поправка 2020 года закрепила, что государство обязано обеспечивать безопасность личности в цифровой среде. И сейчас как раз обсуждается необходимость создания «Цифрового кодекса» — своего рода правил в цифровом пространстве, где права граждан будут в приоритете.

Таким образом, роль больших данных (Big Data) — не в том, чтобы контролировать людей, а в том, чтобы помогать государству. Но для этого нужен баланс: технологии — да, но в рамках закона и с уважением к каждому.

В табл. 2 представлены примеры применения Big Data для защиты социальных прав.

Применяя указанные технологии и методы, различные фонды социальной помощи могут осуществлять адресное сопровождение обеспечения (защиты тех или иных прав граждан). Например, анализируя модели поведения, используемые Big Data могут рассчитывать «коэффициент риска» для каждой заявки на оказание конкретной помощи.

Благодаря этому специалисты фондов получают возможность адресной проверки лишь наиболее подозрительных эпизодов, что заметно экономит их рабочее время. Борьба с хищениями переходит, таким образом, из реактивной плоскости в проактивную — преступление пресекается ещё до того момента, как бюджетные средства окажутся выведенными.

Защитой социальных прав сфера приложения технологий Big Data, разумеется, не исчерпывается. Удобной иллюстрацией здесь служит экологическое законодательство — область, которая, по всей видимости, предоставляет наиболее обширное поле для внедрения цифровых решений.

Существенный перелом наметился с появлением спутникового мониторинга, подкреплённого аналитическим потенциалом Big Data в части обработки изображений. Связка этих технологий позволяет автоматически отслеживать, как меняется состояние лесных массивов, водных объектов и земельных угодий. Несанкционированные свалки, незаконные рубки, аномальные изменения окраски водоемов — индикатор загрязнения — выявляются алгоритмически, без непосредственного участия инспектора. Параллельно работают сети IoT-датчиков, размещенные в окрестностях промышленных предприятий: они фиксируют превышение допустимых концентраций вредных веществ в режиме реального времени. Обращает на себя внимание прикладной эффект подобной интеграции — оперативная реакция правоохранительных органов на деяния, предусмотренные статьями 247–248 УК РФ.

Следует отметить, что, еще в 2020 году президент Российской Федерации В. В. Путин поручил проработать изменения в законодательство с учетом защиты прав граждан при обработке их персональных данных.

В России сейчас активно обсуждаются несколько важных инициатив по совершенствованию законодательства в сфере больших данных.

Одна из ключевых инициатив — разработка законопроекта Минкомсвязью, направленного на правовое регулирование оборота больших данных и защиту персональной информации при их обработке. Сейчас в законодательстве нет отдельного акта, который бы четко регулировал эти процессы. В частности, планируется ввести официальные понятия: «большие данные», «оператор больших данных», «обработка больших данных».

Обсуждается, помимо прочего, и наделение Роскомнадзора правом вести реестр операторов больших данных — мера, которой надлежит обеспечить большую прозрачность отрасли и усилить контроль над нею.

Антимонопольное регулирование составляет ещё одно направление предлагаемых преобразований.

Таблица 2 — Примеры применения Big Data для защиты социальных прав[1]

Сфера защиты прав	Технология и метод	Конкретный механизм воздействия
Право на социальное обеспечение	Predictive Analytics, Data Mining.	Выявление аномалий в данных для профилактики мошенничества с выплатами (например, пересекающиеся получатели, несоответствие декларируемых данных).
Трудовые права	Анализ структурированных и неструктурированных данных.	Мониторинг соблюдения трудового законодательства: выявление признаков дискриминации, неформальной занятости, прогнозирование нарушений охраны труда.
Право на благоприятную окружающую среду	Нейросети для анализа спутниковых снимков, данные с IoT-датчиков.	Круглосуточный мониторинг экологической обстановки; автоматическое обнаружение фактов незаконных выбросов, сбросов или свалок.

[1] Составлено на основании [3; 5; 6].

© Ходусов А. А.

Со стороны экспертов звучит предложение скорректировать законодательство таким образом, чтобы за ФАС закреплялась возможность пресекать использование Big Data в целях упрочения доминирующего положения на рынке. Допустим, крупная компания ограничивает конкурентам доступ к данным либо сводит воедино сведения из различных сервисов, добиваясь тем самым нечестного преимущества, — подобные действия могут получить квалификацию злоупотребления.

Рассматривается также введение особого критерия — доступа к критически важным данным — при оценке того, занимает ли компания доминирующее положение. Для цифровых платформ, где именно данные превращаются в ключевой конкурентный ресурс, соображение это приобретает особую значимость.

Считаем актуальным и использование Big Data для анализа судебной практики. Алгоритмы обработки могут обрабатывать тысячи судебных решений, выявляя противоречия в квалификации одних и тех же деяний.

Заключение

Итак, к основным пробелам и коллизиям законодательства в сфере правового регулирования больших данных (Big Data) можно отнести следующие:

1. Неоднозначность понятий — в законодательстве часто отсутствует четкое определение таких терминов, как «большие данные», «анализ данных», «профилирование». Это затрудняет применение норм права на практике.

2. Противоречие между обработкой Big Data и правом на приватность — сбор, хранение и анализ огромных массивов данных могут нарушать право на неприкосновенность частной жизни. Особенно остро это стоит, когда данные агрегируются из разных источников и позволяют идентифицировать личность, даже если изначально они были анонимными.

3. Проблемы с согласием на обработку персональных данных — в условиях Big Data часто невозможно получить осознанное и конкретное согласие субъекта данных на все возможные цели обработки.

4. Коллизии между отраслевыми законами, например, в здравоохранении, финансах или образовании действуют специальные правила о конфиденциальности, которые могут противоречить возможностям анализа данных на массовой основе.

5. Хранение и передача данных за рубежом — в России действует требование о локализации персональных данных (ФЗ-152), но при работе с Big Data часто требуется кросс-граничный обмен информацией. Это создает юридические риски для компаний.

6. Ответственность за автоматические решения — Big Data часто используются в алгоритмах, принимающих решения (например, в кредитовании или найме). Но если решение ошибочно или дискриминационно — кто несет ответственность: разработчик, оператор, владелец платформы?

7. Недостаток норм о прозрачности и подотчетности — многие алгоритмы анализа данных — «черные ящики».

8. Интеллектуальная собственность на данные и алгоритмы — зачастую отсутствует понимание, кому принадлежат данные, собранные из открытых источников, и кто обладает правами на результаты анализа. Это порождает споры между компаниями и пользователями.

В современных условиях законодательство пока отстает от технологий. За рубежом, например, с этим частично пытаются справиться через GDPR, в России — через развитие ФЗ-152 и обсуждение новых норм в области цифровой экономики. Но системное и всестороннее регулирование Big Data пока отсутствует.

К перспективам использования Big Data для защиты социальных прав граждан в различных сферах законодательства можно отнести:

В сфере здравоохранения — Big Data помогает выявлять системные проблемы в доступе к медпомощи. Например, анализируя данные о том, где и как часто люди не могут попасть к врачу, можно понять, где не хватает поликлиник или специалистов. Это особенно важно для удаленных регионов.

В сфере образования — анализ данных по успеваемости, посещаемости, переходу из школы в вузы. Big Data может помочь выявить, кто находится в группе риска — например, дети из малообеспеченных семей. И тогда государство сможет вовремя вмешаться: дать дополнительную поддержку, запустить программы наставничества или выделить гранты.

В жилищно-коммунальной сфере — система анализирует жалобы жильцов, сроки ремонта, аварии в домах. И вдруг выясняется, что в одном районе коммунальные службы игнорируют людей. Такие паттерны можно выявить только с помощью анализа больших массивов данных.

Список источников

1. Амиянц К. А., Чемеринский К. В. Использование искусственного интеллекта в современной судебной системе и права человека // Международный журнал гуманитарных и естественных наук. 2019. № 11–3. С. 49–52. DOI: 10.24411/2500-1000-2019-11811

2. Атабеков А. Р. Концептуальные подходы и практика правового регулирования искусственного интеллекта в публичной сфере: сравнительно-правовое исследование: автореф. дис. … д-ра. юрид. наук. М. 2024. 40 с.

3. Овездурдыева И. К., Мырадов М. Т. Технологии работы с большими данными «BIG DATA»: сбор, хранение и обработка больших данных // Наука и мировоззрение. 2024. № 29. С. 1–5.

© Ходусов А. А.

4. Бадмаева М. Х. Социально-философские проблемы и принципы применения систем искусственного интеллекта: автореф. дис. … канд. философ. наук. Улан-Удэ 2023. 34 с.

5. Дианова-Клокова И. В., Метаньев Д. А. О некоторых тенденциях пространственного развития социального инжиниринга научно-инновационной деятельности // Academia. Архитектура и строительство. 2021. № 3. С. 41–49. DOI: 10.22337/2077-9038-2021-3-41-49

6. Лаушкина О. С. Роль искусственного интеллекта в автоматизации процессов социального обеспечения в России // Вестник науки. 2025. № 11 (92). С. 223–228.

7. Фаллетти Э. Алгоритмическая дискриминация и защита неприкосновенности частной жизни // Journal of Digital Technologies and Law. 2023. № 2. С. 387–420. DOI: 10.21202/jdtl.2023.16

8. Пильгун М. А. Прогнозная аналитика и образы будущего по данным социальных медиа // Медиалингвистика. 2025. Т. 12, № S. С. 800–804.

9. Соколова А. Ю. Защита прав потребителей и дискриминация при использовании ценовых алгоритмов // Вестник науки. 2025. № 11 (92). С. 292–301.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Ходусов Алексей Александрович

Кандидат юридических наук, доцент, заведующий кафедрой уголовно-правовых дисциплин, Международный юридический институт (Москва, Россия).
E-mail: yustas-73@mail.ru

INFORMATION ABOUT THE AUTHOR

Alexey A. Khodusov

Candidate of Legal Sciences, Associate Professor,
Head of the Department of Criminal Law Disciplines, International Law Institute (Moscow, Russia)
E-mail: yustas-73@mail.ru

КОНФЛИКТ ИНТЕРЕСОВ

Конфликт интересов отсутствует.

CONFLICT OF INTEREST

There is no conflict of interest.

Дата поступления статьи / Received: 22.06.2026.
Дата рецензирования статьи / Revised: 25.07.2026.
Дата принятия статьи к публикации / Accepted: 27.07.2026.

© Ходусов А. А.