

ЦИФРОВОЕ ПРАВО

Дата поступления рукописи в редакцию: 11.06.2026 г.

DOI: 10.24412/2076-1503-2026-8-795-799

Дата принятия рукописи в печать: 02.07.2026 г.

КИРИЛЛОВА Татьяна Константиновна,

Профессор кафедры гражданского права, д.ю.н., профессор
Санкт-Петербургского государственного университета
аэрокосмического приборостроения,
e-mail: tania.kirillova@gmail.com@yandex.ru

**НЕЙРОСЕТИ И ПРАВО НА НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ
ЖИЗНИ**

Аннотация. В статье исследуются теоретические и правовые аспекты влияния нейросетевых технологий на реализацию конституционного права на неприкосновенность частной жизни. Показано, что современные нейросети выступают не только инструментом автоматизации аналитических процессов, но и источником качественно новых рисков, связанных с масштабным извлечением, сопоставлением и выводом сведений о личности, её поведении, привычках, круге общения и биометрических характеристиках.

Особое внимание уделяется правовым последствиям обучения нейросетей на массиве персональных данных, проблеме вторичного использования сведений, угрозам деанонимизации, а также рискам возникновения автоматизированной дискриминации и необоснованного профилирования граждан. Анализируются положения Конституции Российской Федерации, федеральных законов об информации, персональных данных, государственных услугах и биометрической аутентификации, а также доктринальные подходы к защите частной жизни в цифровую эпоху. На основе исследования делается вывод о необходимости выработки специального правового режима применения нейросетей, основанного на принципах законности, пропорциональности, прозрачности и минимизации данных.

Ключевые слова: нейросети, искусственный интеллект, неприкосновенность частной жизни, персональные данные, биометрические данные, цифровизация, автоматизированная обработка, права человека.

KIRILLOVA Tatyana Konstantinovna,

Professor of the Department of Civil Law, Doctor of Law, Professor
at the St. Petersburg State University of Aerospace Instrumentation

NEURAL NETWORKS AND THE RIGHT TO PRIVACY

Annotation. The article examines the theoretical and legal aspects of how neural network technologies affect the constitutional right to privacy. It shows that modern neural networks are not merely tools for automating analytical tasks, but also a source of qualitatively new risks associated with the large-scale extraction, comparison and inference of information about a person, including behaviour, habits, social ties and biometric characteristics.

Particular attention is paid to the legal consequences of training neural networks on large volumes of personal data, the problem of secondary use of information, the risks of de-anonymisation, and the emergence of automated discrimination and unjustified profiling of citizens. The article analyzes the provisions of the Constitution of the Russian Federation, federal laws on information, personal data, public services and biometric authentication, as well as doctrinal approaches to the protection of privacy in the digital age. The study concludes that a special legal regime for neural network use is necessary, based on legality, proportionality, transparency and data minimization.

Key words: neural networks, artificial intelligence, privacy, personal data, biometric data, digitalization, automated processing, human rights.

Цифровая трансформация привела к тому, что значительная часть повседневной активности человека стала оставлять устойчивые информационные следы, которые могут быть собраны, сопоставлены и интерпретированы алгоритмами без непосредственного участия самого субъекта. В условиях, когда нейросети способны выявлять связи между несопоставимыми на первый взгляд фрагментами данных, право на неприкосновенность частной жизни приобретает новое содержание и перестает сводиться только к запрету прямого вмешательства в личную сферу человека [6].

Если традиционное понимание частной жизни строилось вокруг охраны жилища, переписки, семейной тайны и личной автономии, то в цифровую эпоху к этим объектам добавляются поведенческие модели, цифровые профили, прогностические выводы и результаты машинного анализа, которые часто оказываются не менее чувствительными, чем исходные сведения. Именно нейросети позволяют извлекать из больших массивов информации скрытые закономерности, вследствие чего даже обезличенные данные могут быть использованы для повторной идентификации лица или для построения его вероятностного портрета [9].

В научной литературе неоднократно подчеркивалось, что развитие цифровых технологий повышает качество административных, коммерческих и сервисных решений, однако одновременно ослабляет традиционные механизмы контроля над личной информацией. Так, Г.Е. Волкова отмечает, что право на неприкосновенность частной жизни в цифровую эпоху должно пониматься как право личности сохранять контроль над обращением сведений о себе, а не только как защита от физического проникновения в личное пространство [6].

В настоящей статье нейросети рассматриваются как особый вид интеллектуальных систем, способных не только обрабатывать информацию, но и генерировать выводы, влияющие на юридически значимые решения. Это делает необходимым исследование вопроса о том, при каких условиях использование нейросетей допустимо с точки зрения конституционных гарантий частной жизни, а при каких оно превращается в чрезмерное и несоразмерное вмешательство в сферу личной автономии гражданина.

Методологическую основу исследования составили формально-юридический, системный, сравнительно-правовой и доктринальный методы. Их применение позволило рассмотреть нейросети одновременно как технологический инструмент, как механизм обработки информации и как фактор трансформации правового режима частной жизни.

Нормативную базу исследования составля-

ют Конституция Российской Федерации, закрепляющая право каждого на неприкосновенность частной жизни, личную и семейную тайну, защиту чести и доброго имени, а также право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений [1]. Существенное значение имеют Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» и Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» [2-4].

Отдельное место занимает Федеральный закон от 29.12.2022 № 572-ФЗ, который регулирует идентификацию и аутентификацию физических лиц с использованием биометрических персональных данных и тем самым закрепляет новую модель правового обращения чувствительной информации о человеке [5]. Именно этот массив норм важен для исследования нейросетей, поскольку современные нейросетевые решения нередко используют биометрические, поведенческие и контекстуальные данные одновременно, формируя многоуровневую цифровую среду наблюдения.

Доктринальная база включает исследования о праве на неприкосновенность частной жизни в цифровую эпоху, об алгоритмической дискриминации, о безопасности частной жизни при взаимодействии с генеративным искусственным интеллектом, о влиянии больших данных на частную жизнь, а также о биометрической идентификации в интернете [6]. Сопоставление указанных работ позволило выявить общую тенденцию: риск для частной жизни возрастает не только при прямом сборе данных, но и при их анализе, классификации и выводе скрытых характеристик личности.

Право на неприкосновенность частной жизни в контексте нейросетей следует понимать как совокупность правовых возможностей лица контролировать получение, хранение, анализ, интерпретацию и распространение сведений, относящихся к его личной сфере. В отличие от классических схем обработки информации, нейросеть не просто хранит или передает данные: она строит вероятностные модели поведения, обнаруживает связи и формирует предсказания, которые могут оказывать прямое влияние на доступ к услугам, кредитам, медицинской помощи, образованию и другим благам [7].

Наиболее очевидным источником правового риска является обучение нейросетей на больших массивах данных, включая тексты, изображения, аудиозаписи и видеоматериалы. Даже при наличии заявленной анонимизации пользователь-

ских данных сохраняется возможность повторной идентификации лица через сопоставление цифровых следов, контекстных маркеров и устойчивых поведенческих паттернов. А.П. Иванова справедливо указывает, что в эпоху больших данных традиционные механизмы защиты персональных данных теряют эффективность, поскольку анализ массивов информации сам по себе способен раскрывать сведения, ранее не воспринимавшиеся как конфиденциальные [9].

Для нейросетей особенно характерен феномен вторичного использования данных: сведения, переданные для одной цели, затем применяются для обучения модели, последующего тестирования, улучшения качества сервиса или коммерческой аналитики. При таком подходе согласие субъекта становится формальным и мало что значит, если человек не понимает ни объема собираемых данных, ни реальных направлений их дальнейшего применения. В научной литературе это рассматривается как одна из наиболее острых проблем современной цифровой экономики и как фактор ослабления конфиденциальности [6].

Особую опасность представляют нейросети, работающие с биометрическими данными: изображением лица, голосом, манерой речи, походкой, а в перспективе - с комплексными поведенческими признаками. Федеральный закон № 572-ФЗ создал специальные правила идентификации и аутентификации с использованием биометрии, однако сам по себе не снимает вопроса о допустимости чрезмерного расширения сфер применения таких технологий [5]. Биометрия способна усиливать как удобство сервиса, так и риск необратимого раскрытия личности, а потому требует максимально строгих гарантий доступа, хранения и передачи данных [11].

Нейросети также меняют характер частно-правовых и публично-правовых отношений. Если раньше вмешательство в частную жизнь было связано в основном с незаконным сбором информации или ее разглашением, то сегодня к вмешательству следует относить и автоматизированное профилирование, и скрытое ранжирование пользователей, и создание поведенческих прогнозов. Э. Фаллетти, анализируя алгоритмическую дискриминацию, показывает, что алгоритмы способны воспроизводить и усиливать социальные неравенства, когда решение о человеке принимается на основе статистического сходства, а не его индивидуальных качеств [7].

В связи с этим особое значение приобретает принцип прозрачности. Лицо должно знать не только о самом факте обработки его данных, но и о логике, целях и последствиях применения нейросети. Без такого понимания право на неприкос-

новенность частной жизни превращается в декларацию, не обеспеченную реальным механизмом защиты. Именно поэтому в современных правовых подходах усиливается внимание к оценке алгоритмов, к аудиту моделей и к обязательствам оператора объяснять происхождение юридически значимых выводов [6].

Еще одним направлением риска становится использование нейросетей в системах наблюдения, распознавания лиц и поведенческого анализа. Совмещение видеопотоков, биометрических идентификаторов и массивов дополнительных сведений позволяет создавать практически непрерывный контроль за передвижением и повседневной активностью человека. Такой контроль затрагивает не только право на частную жизнь, но и свободу выражения мнений, свободу собраний и право на автономию личности, поскольку осознание постоянного наблюдения оказывает сдерживающее воздействие на поведение гражданина [10].

Не менее сложной является проблема использования нейросетей в сфере государственных и муниципальных услуг. С одной стороны, автоматизация ускоряет обслуживание и сокращает административные издержки; с другой стороны, ошибка в модели, неверная классификация или некорректный вывод могут привести к отказу в услуге, ограничению доступа к информации либо к необоснованному подозрению в отношении гражданина. В подобных случаях необходимы не только формальные гарантии, но и механизмы человеческого контроля над машинным решением, поскольку именно человек остается носителем прав и обязанностей [4].

Отдельного внимания заслуживает вопрос о том, подлежит ли нейросетевая модель как таковая правовой охране или правовому ограничению. На наш взгляд, сама нейросеть не может рассматриваться как субъект права и не должна заслонять собой человека в юридической конструкции. Значение имеет не модель как технический объект, а последствия ее работы: какой объем данных использован, была ли соблюдена законная цель обработки, существует ли минимизация сведений и можно ли оспорить полученный результат [3].

При анализе нейросетей необходимо различать допустимую автоматизацию и недопустимую подмену правового решения машинным выводом. Если нейросеть помогает фильтровать спам, повышать кибербезопасность или обнаруживать технические ошибки, ее применение может быть оправдано. Однако если модель формирует скрытые профили личности, прогнозирует уязвимость, эмоциональное состояние или вероятность поведения без ясного правового основания, возникает риск несоразмерного вмешательства в частную

жизнь, которое не может быть признано допустимым только на том основании, что оно удобно для оператора [8].

Т.А. Костылева и А.М. Кондаков, исследуя цифровую идентичность, убедительно показали, что цифровой профиль формируется как совокупность идентификационных и поведенческих данных, а значит, любые технологии, усиливающие профилирование человека, должны оцениваться через призму прав личности на контроль над собственной цифровой проекцией [6]. Этот вывод полностью применим и к нейросетям, поскольку именно они наиболее активно конструируют вероятностные образцы поведения и тем самым создают новую форму влияния на личную сферу.

Правовой режим в рассматриваемой сфере должен строиться на нескольких базовых принципах: законность обработки, ограничение целей, минимизация данных, прозрачность алгоритмов, недопустимость скрытого сопоставления сведений и наличие эффективной процедуры обжалования решений, основанных на нейросетевом анализе. В противном случае право на неприкосновенность частной жизни будет существовать лишь формально, а реальный контроль над сведениями о человеке перейдет к владельцам платформ, разработчикам моделей и операторам данных [9].

Проведенное исследование позволяет сделать вывод о том, что нейросети являются одним из наиболее значимых факторов трансформации права на неприкосновенность частной жизни в XXI веке, поскольку они позволяют не только собирать и хранить сведения, но и извлекать из них новые, ранее скрытые характеристики личности.

Главная правовая проблема состоит в том, что нейросети способны работать с массивами данных таким образом, что граница между публичной и частной информацией становится все менее определенной, а потому традиционные механизмы охраны конфиденциальности нуждаются в существенном обновлении.

Нейросетевые технологии допустимы при условии строгого соблюдения принципов законности, пропорциональности, минимизации, прозрачности и подотчетности, а также при наличии эффективных процедур контроля и обжалования машинных решений, затрагивающих права граждан.

В целях совершенствования законодательства представляется необходимым закрепить специальные требования к обучению и эксплуатации нейросетей, которые обрабатывают персональные и биометрические данные, установить обязанность информирования граждан о целях и логике анализа сведений, а также предусмотреть действенные санкции за скрытое профилирование и неправомерное вторичное использование

информации.

Список литературы:

[1] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Российская газета. 1993. 25 декабря. № 237; Российская газета. 2020. 4 июля. № 144.

[2] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации. 2006. № 31. Ст. 3448.

[3] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации. 2006. № 31. Ст. 3451.

[4] Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» // Собрание законодательства Российской Федерации. 2010. № 31. Ст. 4179.

[5] Федеральный закон от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» // Собрание законодательства Российской Федерации. 2023. № 1 (ч. I). Ст. 19.

[6] Волкова Г.Е. Право на неприкосновенность частной жизни в цифровую эпоху // Философия права. 2022. № 4 (103). С. 174–180.

[7] Фаллетти Э. Алгоритмическая дискриминация и защита неприкосновенности частной жизни // Journal of Digital Technologies and Law. 2023. Т. 1, № 2. С. 387–420. DOI: 10.21202/jdtl.2023.16.

[8] Титов М.Д., Назаров Д.М. Безопасность частной жизни человека при взаимодействии с генеративным искусственным интеллектом // Современные инновации, системы и технологии. 2023. Т. 3, № 4. С. 342–348. DOI: 10.47813/2782-2818-2023-3-4-0342-0348..

[9] Иванова А.П. Большие данные и право на неприкосновенность частной жизни // Социальные и гуманитарные науки. Отечественная и зарубежная литература: ИАЖ. Сер. Государство и право. 2024. № 4. С. 149–163. DOI: 10.31249/iajpravo/2024.04.12..

[10] Кузнецова С.С., Мочалов А.Н., Саликов М.С. Биометрическая идентификация в интернете: тенденции правового регулирования в России и за рубежом // Вестник Томского государственного

университета. 2022. № 476. С. 257–267. DOI: 10.17223/15617793/476/28..

[11] Смирнова Я.В. Проблемы обеспечения права на охрану частной жизни при обработке биометрических данных в Европейском союзе // Актуальные проблемы российского права. 2022. Т. 17, № 10 (143). С. 183–192. DOI: 10.17803/1994-1471.2022.143.10.183-192..

References:

[1] The Constitution of the Russian Federation (adopted by popular vote 12.12.1993 with amendments approved during the all-Russian vote 01.07.2020) // Rossiyskaya Gazeta. 1993. December 25. № 237; Russian newspaper. 2020. July 4th. № 144.

[2] Federal Law of 27.07.2006 No. 149-FZ "On Information, Information Technologies and Information Protection" // Collection of Legislation of the Russian Federation. 2006. № 31. Art. 3448.

[3] Federal Law of 27.07.2006 No. 152-FZ "On Personal Data" // Collection of Legislation of the Russian Federation. 2006. № 31. Art. 3451.

[4] Federal Law of 27.07.2010 No. 210-FZ "On the Organization of the Provision of State and Municipal Services" // Collection of Legislation of the Russian Federation. 2010. № 31. Art. 4179.

[5] Federal Law of 29.12.2022 No. 572-FZ "On the Identification and (or) Authentication of Individuals Using Biometric Personal Data, on Amending Certain

Legislative Acts of the Russian Federation and Invalidating Certain Provisions of Legislative Acts of the Russian Federation" // Collection of Legislation of the Russian Federation. 2023. No. 1 (part I). Art. 19.

[6] Volkova G.E. The right to privacy in the digital age // Philosophy of law. 2022. № 4 (103). S. 174-180.

[7] Falletti E. Algorithmic Discrimination and Privacy Protection // Journal of Digital Technologies and Law. 2023. T. 1, NO. 2. S. 387-420. DOI: 10.21202/jdtl.2023.16.

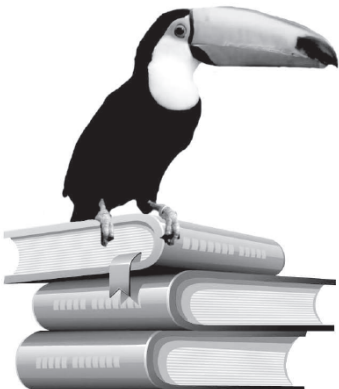
[8] Titov M.D., Nazarov D.M. Security of human privacy in interaction with generative artificial intelligence // Modern innovations, systems and technologies. 2023. T. 3, NO. 4. S. 342-348. DOI: 10.47813/2782-2818-2023-3-4-0342-0348..

[9] Ivanova A.P. Big Data and the Right to Privacy // Social Sciences and Humanities. Domestic and foreign literature: IAZH. Ser. State and law. 2024. № 4. S. 149-163. DOI: 10.31249/iajpravo/2024.04.12..

[10] Kuznetsova S.S., Mochalov A.N., Salikov M.S. Biometric identification on the Internet: trends in legal regulation in Russia and abroad // Bulletin of Tomsk State University. 2022. № 476. PP. 257-267. DOI: 10.17223/15617793/476/28..

[11] Smirnova Y.V. Problems of ensuring the right to privacy when processing biometric data in the European Union // Current problems of Russian law. 2022. T. 17, NO. 10 (143). S. 183-192. DOI: 10.17803/1994-1471.2022.143.10.183-192..





Юридическое издательство
«ЮРКОМПАНИ»

Издание учебников,
учебных и методических
пособий, монографий,
научных статей.

Профессионально.

В максимально
короткие сроки.

Размещаем
в РИНЦ, Е-Library.

ЮРКОМПАНИ

www.law-books.ru