

DOI: 10.17803/2542-2472.2026.38.2.014-025

СОГЛАСИЕ НА ОБРАБОТКУ БИОМЕТРИЧЕСКИХ ПЕРСОНАЛЬНЫХ ДАННЫХ ГЕНЕРАТИВНЫМ ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ: ПРОБЛЕМЫ ПРАКТИЧЕСКОЙ РЕАЛИЗАЦИИ

Печенин Даниила Вячеславович,
магистрант направления «Цифровое право (IT-Law)»
Университета имени О.Е. Кутафина (МГЮА)
125993, Россия, г. Москва, Садовая-Кудринская ул., д. 9
s2039817@edu.msal.ru

© Печенин Д. В., 2026

Аннотация. В статье рассматривается соответствие законодательству РФ процесса обработки биометрических персональных данных в системах генеративного ИИ, проводится сравнение правового регулирования данных отношений в России и ЕС. Выявлены системные пробелы в реализации правомерной обработки биометрических персональных данных системами генеративного искусственного интеллекта. Установлено, что запреты на использование биометрических персональных данных в запросах носят декларативный характер, это подтверждается анализом политик конфиденциальности GigaChat и DeepSeek, возлагающих ответственность за неправомерное использование персональных данных на пользователя. Непрозрачный механизм получения согласия субъекта на обработку биометрических персональных данных и обусловленность доступа к сервису их обязательной обработкой для обучения нейронной сети представляются главными проблемами реализации правомерной обработки данных системами генеративного искусственного интеллекта. На основе сравнительного анализа российского и европейского законодательства сформулированы следующие предложения: 1) закрепить императивный запрет на обработку биометрических персональных данных системами генеративного искусственного интеллекта с установлением юридической ответственности либо обязать операторов систем генеративного искусственного интеллекта внедрять меры верификации письменных согласий субъектов на обработку; 2) обработка биометрических персональных данных исключительно для целей обучения нейронных сетей должна производиться с отдельного информированного согласия субъекта, без которого использование сервиса должно оставаться невозможным. Предложенные меры направлены на устранение противоречий, обеспечение реального контроля субъектов над своими биометрическими персональными данными и их правовой защиты.

Ключевые слова: биометрические персональные данные; согласие на обработку персональных данных; субъект персональных данных; оператор; генеративный искусственный интеллект; правовое регулирование; Европейский Союз; нейросеть; биометрия

CONSENT FOR PROCESSING BIOMETRIC PERSONAL DATA BY GENERATIVE AI: PRACTICAL IMPLEMENTATION PROBLEMS

Daniil V. Pechenin,

Master's Student, IT-Law Master's Course, Kutafin Moscow State Law University (MSAL)
s2039817@edu.msall.ru

Abstract. The paper examines the compliance of biometric personal data processing in generative AI systems with the legislation of the Russian Federation and provides a comparative analysis of the legal regulation of relations under examination in Russia and the European Union. The study identifies systemic gaps in ensuring the lawful processing of biometric personal data by generative artificial intelligence systems. The study has established that prohibitions on the use of biometric personal data in user prompts are largely declaratory in nature, as evidenced by an analysis of the privacy policies of GigaChat and DeepSeek, which place responsibility for the unlawful use of personal data on the user. The opaque mechanism for obtaining a data subject's consent to the processing of biometric personal data, as well as conditioning access to the service on the mandatory processing of such data for neural network training purposes, appear to constitute the principal challenges to ensuring lawful data processing by generative artificial intelligence systems. Based on a comparative analysis of Russian and European legislation, the author proposes the following: (1) to establish a mandatory prohibition on the processing of biometric personal data by generative AI systems, coupled with the imposition of legal liability, or alternatively to require operators of generative artificial intelligence systems to implement mechanisms for verifying the existence of the data subject's written consent to processing; and (2) to require that the processing of biometric personal data exclusively for neural network training purposes be carried out only on the basis of separate informed consent of the data subject, while access to the service should remain possible even in the absence of such consent. The proposed measures are aimed at eliminating existing contradictions, ensuring genuine control by data subjects over their biometric personal data, and strengthening their legal protection.

Keywords: biometric personal data; consent to the processing of personal data; personal data entity; operator; generative artificial intelligence; legal regulation; European Union; neural network; biometrics

ВВЕДЕНИЕ

Искусственный интеллект (ИИ) уже вышел за рамки «перспективы» и превратился в повседневный инструмент для бизнеса, государства, гражданина. Его активно применяют в образовании, маркетинге, анализе поведения клиентов, системах скоринга, в кол-центрах, генерации текстов, изображений, видео и аудио — 70 % всех компаний в РФ¹. В 2025 г. 51 % интернет-пользователей обращались к нейросетям, а рынок генеративного ИИ в РФ прогнозировал рост в 5 раз до 58 млрд руб. по сравнению с показателями 2024 г.² ИИ обрабатывает входные данные и генерирует материал посредством нейронной сети, которая обучается на заранее заданных для нее паттернах. В результате такой обработки формируется база данных, которая генерирует

¹ Российский рынок генеративного ИИ в 2025 году вырастет в 5 раз и достигнет 58 миллиардов из-за колоссального спроса // CNews. 2025. 9 дек. URL: https://www.cnews.ru/news/top/2025-12-09_v_2025_godu_rossijskij_rynok (дата обращения: 26.12.2025).

² Нейросети: инструмент, а не магия // Всероссийский центр исследования общественного мнения. URL: <https://wciom.ru/analytical-reviews/analiticheskii-obzor/neiroseti-instrument-a-ne-magija> (дата обращения: 26.12.2025).

ответ, приближенный к тому, который смог бы дать человек. Для обработки персональных данных (ПД) субъекта при создании промптов в системах генеративного ИИ, в том числе и при дальнейшем их использовании для обучения нейронных сетей, обязательно наличие согласия на обработку ПД. Однако в отношении биометрических персональных данных (БПД или биометрия) — наиболее чувствительной категории, характеризующей физиологические и биологические особенности человека согласно п. 1 ст. 11 Федерального закона № 152-ФЗ «О персональных данных»³ (далее — Федеральный закон № 152-ФЗ) данное согласие носит общий, формальный характер. Кроме того, такое согласие не предполагает автоматического разрешения на использование биометрии в обучении — поскольку эти процессы обычно выходят за рамки первоначально указанных целей и требуют отдельной информированности субъекта. Биометрия, включая изображения лица, голосовые записи, радужку глаза, отпечатки пальцев и др. не подлежит восстановлению или изменению, что делает ее необратимой и усиливает риски при генеративной обработке: от создания дипфейков до бесконтрольного синтеза «новых» генеративных объектов на основе БПД, способных нанести вред репутации, приватности или даже идентичности субъекта. Учитывая тот факт, что уже в 2023 г. было собрано 75 млн образцов лица и голоса в российских организациях⁴, прослеживается очевидный масштаб отрасли, спрос на большие объемы данных и важность правового регулирования и обеспечения правовых механизмов защиты БПД в сфере ИИ.

Стратегическую важность обеспечения безопасности в обработке ПД видит Президент РФ В. В. Путин. На заседании Совета по развитию гражданского общества и правам человека 9 декабря 2025 г. президент отметил необходимость развивать сферы ИИ и big data, обеспечивая гарантии безопасности прав человека, чтобы не допустить бездумного использования ИИ и «распыления идентичности россиян»⁵. Регламент (ЕС) 2016/679⁶ (GDPR) дополняется Регламентом ЕС 2024/1689⁷ (AI Act) строгими требованиями к управлению данными для высокорисковых систем, включая отзыв согласия, но российское правовое регулирование ИИ остается фрагментарным, порождая пробелы в защите фундаментального права на неприкосновенность частной жизни⁸.

³ Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 24.06.2025) «О персональных данных» // СЗ РФ. 2006. № 31 (ч. 1). Ст. 3451.

⁴ Пароль не нужен: что нужно знать о биометрии // Объясняем.пф. URL: <https://объясняем.пф/articles/useful/biometricheskie-dannye-chto-nuzhno-znat/> (дата обращения: 26.12.2025).

⁵ Путин выступил против бездумного использования ИИ // Hi-Tech Mail. URL: <https://hi-tech.mail.ru/news/138948-putin-vystupil-protiv-bezdumnogo-ispolzovaniya-ii/> (дата обращения: 26.12.2025).

⁶ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) // URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng> (дата обращения: 28.12.2025).

⁷ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Artificial Intelligence Act // URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689> (дата обращения: 28.12.2025).

⁸ Кутейников Д. Л., Ижаев О. А., Алексеевич Л. В., Зенин С. С. Неприкосновенность частной жизни в условиях использования систем искусственного интеллекта для удаленной биометрической идентификации личности // Lex russica. 2022. Т. 75. № 2. С. 121–131.

1. ИНСТИТУТ СОГЛАСИЯ НА ОБРАБОТКУ БПД: ЕГО НАЗНАЧЕНИЕ И СОВРЕМЕННОЕ ПРАВОВОЕ РЕГУЛИРОВАНИЕ В РФ

Сведения об определяемом или определенном лице составляют его неотъемлемую индивидуальность, когда речь идет о биометрии. Отдельные сведения, которые порой идентичны, как, например имя, фамилия, возраст, пол, не приводят к идентификации конкретного человека, являются абстрактными, а потому, строго говоря, не затрагивают право на неприкосновенность частной жизни. Можно, как справедливо отмечает М. Б. Добробаба, вывести правило по тесту: если сведения изначально сами по себе не приводят нас к заключению, что это ПД, но в совокупности с иными сведениями мы сможем верифицировать лицо, то эти сведения относятся к ПД⁹.

Бесконтрольное использование ПД, овладение ими влечет за собой большие юридические риски, обусловленные возможностью их использования в преступных целях, завладение банковскими счетами, мошенничество, шантаж и другие неблагоприятные последствия. Поэтому институт согласия на обработку ПД реализует функцию по защите от несанкционированного использования ПД третьими лицами и предупреждает совершение преступлений или правонарушений в сфере их обработки.

Основным источником правового регулирования обработки БПД является Федеральный закон № 152-ФЗ, в котором главным основанием их обработки является согласие субъекта, полученное в письменном виде, за исключением специально предусмотренных законом случаев. Название этой категории происходит от греч. *bios* — жизнь, и *metron* — мера¹⁰. Некоторые авторы отмечают, что в отдельных случаях происходит открытое столкновение человека и машины в борьбе за свои права на использование голоса, поскольку обработка ИИ голосовых данных без надлежащего правового основания недопустима¹¹. Кроме классических физиологических и биологических сведений ГОСТ Р ИСО/ТО 13569-2007 «Финансовые услуги. Рекомендации по информационной безопасности»¹², равно как и Н. И. Платонова¹³, включают в определение БПД также сведения о поведенческих особенностях человека. К поведенческим особенностям можно отнести походку, почерк, манеру набора текста со свойственной данному лицу скоростью и силой нажатия на клавиши клавиатуры или смартфона, эмоции, мимику, характер человека и многое другое. В одном из своих разъяснений Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее — Роскомнадзор)

⁹ Цит. по: Добробаба М. Б. Понятие персональных данных: проблема правовой определенности // Вестник Университета имени О.Е. Кутафина (МГЮА). 2023. № 2. С. 42–52. DOI: 10.17803/2311-5998.2023.102.2.042-052.

¹⁰ Словарь иностранных слов, вошедших в состав русского языка : материалы для лексической разработки заимствованных слов в рус. лит. речи : с портр. и краткой биогр. А. Н. Чудинова / сост. под ред. А. Н. Чудинова. 3-е изд., тщательно испр. и знач. доп. (более 5 000 новых слов) преимущественно соц.-полит. терминами, вошедшими в жизнь в последние годы. СПб. : В. И. Губинский, 1910.

¹¹ Жужгина А. А., Соловьева Д. Д. Правовое регулирование синтеза человеческого голоса с помощью технологий искусственного интеллекта // Вестник ННГУ. 2024. № 5. URL: <https://cyberleninka.ru/article/n/pravovoe-regulirovanie-sinteza-chelovecheskogo-golosa-s-pomoschyu-tehnologiy-iskusstvennogo-intellekta> (дата обращения: 03.01.2026).

¹² ГОСТ Р ИСО/ТО 13569-2007 «Финансовые услуги. Рекомендации по информационной безопасности» : нац. стандарт Российской Федерации : утвержден и введен в действие приказом Федер. агентства по техн. регулированию и метрологии от 27.12.2007 № 514-ст (Система стандартов по информации, библиотечному и издательскому делу) // Кодекс: электрон. фонд правовой и норматив.-техн. информ. URL: <https://docs.cntd.ru/document/1200068821> (дата обращения: 29.12.2025).

¹³ Платонова Н. И. Современный подход к пониманию персональных данных // Право и современные государства. 2017. № 5. URL: <https://cyberleninka.ru/article/n/sovremennyy-podhod-k-ponimaniyu-personalnyh-dannyh> (дата обращения: 06.01.2026).

отмечает, что возможность отнесения тех или иных сведений к БПД регулируется законодательными и иными нормативными правовыми актами¹⁴. Так, согласно п. 6 Перечня персональных данных, записываемых на электронные носители информации, содержащиеся в основных документах, удостоверяющих личность гражданина Российской Федерации, по которым граждане Российской Федерации осуществляют выезд из Российской Федерации и въезд в Российскую Федерацию, утвержденного постановлением Правительства РФ 04.03.2010 № 125 «О перечне персональных данных, записываемых на электронные носители информации, содержащиеся в основных документах, удостоверяющих личность гражданина Российской Федерации, по которым граждане Российской Федерации осуществляют выезд из Российской Федерации и въезд в Российскую Федерацию»¹⁵, цветное цифровое фотографическое изображение лица владельца документа относят к БПД.

Из этого следует, что согласие на обработку БПД является главным правовым основанием их обработки, а получение такого согласия — чрезвычайно важным критерием законности, справедливости, достаточности, точности ПД и соответствия заявленным целям обработки.

2. ИЗМЕНЕНИЯ ЗАКОНОДАТЕЛЬСТВА В ЧАСТИ СБОРА СОГЛАСИЯ НА БПД

Новые положения законодательства о ПД были внесены в 2025 г. Федеральным законом от 24.06.2025 № 156-ФЗ «О создании многофункционального сервиса обмена информацией и о внесении изменений в отдельные законодательные акты Российской Федерации»¹⁶ внесена поправка в текст ст. 9 Федерального закона № 152-ФЗ: с 1 сентября 2025 г. согласие субъекта на обработку ПД оформляется в виде самостоятельного документа. Данное нововведение исключает возможность включения согласия в тексты договоров, оферт или пользовательских соглашений. Установленное требование в полной мере распространяется на обработку БПД, что де-факто прекращает практику так называемого скрытого согласия, при которой волеизъявление на обработку ПД неотделимо от иных юридически значимых действий субъекта. В отношении БПД сохраняется требование письменной формы согласия, предусматривающего указание конкретных целей обработки, перечня совершаемых действий, сроков хранения и использования БПД, а также круга операторов и иных лиц, которым такие данные могут быть переданы.

Федеральным законом от 08.08.2024 № 233-ФЗ «О внесении изменений в Федеральный закон “О персональных данных” и Федеральный закон “О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве и внесении изменений в ст. 6 и 10 Федерального закона “О персональных данных”»¹⁷ введена статья 13.1 в Федеральный закон № 152-ФЗ, которая посвящена особенностям обработки ПД, полученных в результате обезличивания. Теперь операторы по требованию уполномоченного государственного органа передают обрабатываемые ПД в государственную информационную систему, на основе которых создаются специальные составы данных и определяется доступ к ним. Данные внутри этого состава подлежат обезличиванию. К ним имеют доступ не только уполномоченные государственные органы, но также граждане и юридические лица, соответствующие требованиям, установленным пунктом 2 ч. 7 ст. 13.1 Федерального закона № 152-ФЗ. Таким образом, новые положения, регулирующие процессы обезличивания ПД,

¹⁴ Письмо Роскомнадзора от 01.08.2024 № 62450-02-11/77 «Об обработке биометрических персональных данных» // URL: https://www.consultant.ru/document/cons_doc_LAW_483102/ (дата обращения: 29.12.2025).

¹⁵ СЗ РФ. 2010. № 10. Ст. 1103.

¹⁶ СЗ РФ. 2025. № 26 (ч. I). Ст. 3486.

¹⁷ СЗ РФ. 2024. № 33 (ч. I). Ст. 4929.

способствуют развитию технологий ИИ, обработки больших данных в РФ. Введение данных норм предоставляет операторам возможность использовать обезличенные массивы данных для обучения систем ИИ при одновременном соблюдении требований законодательства о ПД. Однако важно иметь в виду, что в такие составы ПД в государственной информационной системе не может входить категория БПД (ч. 1 ст. 13.1 Федерального закона № 152). Из этого следует, что БПД не могут быть использованы даже в обезличенном виде в целях обучения систем ИИ. В данном контексте хотим обратиться к мнению А. С. Селюк, которая обозначает угрозы, которые несут с собой модели машинного обучения и дипфейк для обработки больших данных. Автор верно указывает на уязвимости для БПД и необходимость новых стандартов¹⁸.

Последние нововведения демонстрируют возрастание интереса законодателя к точечным вопросам правового регулирования в сфере обработки БПД, понимание важности института согласия на обработку БПД и стратегического значения регулирования общественных отношений в данном направлении.

3. ТЕХНОЛОГИЯ ОБРАБОТКИ БПД ГЕНЕРАТИВНЫМ ИИ

Исходя из Национальной стратегии развития искусственного интеллекта на период до 2030 года, утвержденной Указом Президента РФ от 10.10.2019 № 490¹⁹, генеративный ИИ определяется через термин большой генеративной модели как модели ИИ, интерпретирующей большие массивы данных в виде текстовой информации или данные об объектах на изображениях, и способной на их основе создать новые мультимодальные данные, на уровне, сопоставимом или превосходящем интеллектуальную деятельность человека. Важное замечание, что такая модель ИИ способна генерировать новые данные в виде изображения, аудио или видео контента, на основе анализа обширных обучающих наборов. Сбор данных ИИ отличается массовостью и автоматизацией, часто через cookies и big data, что затрудняет контроль субъектом. К технологиям ИИ для обработки ПД относятся машинное обучение (ML), системы распознавания вроде Google DeepMind, Siri, Alexa²⁰.

Обратимся к политикам конфиденциальности некоторых систем генеративного ИИ. В частности, российская система генеративного ИИ Сервис GigaChat от ПАО «Сбербанк» (далее — Банк) на основании Пользовательского соглашения об использовании Сервиса GigaChat²¹ (далее — Соглашение) запрещает использовать Пользователю в Запросах в целях генерации контента собственные ПД и другие данные третьих лиц (п. 4.5.6 Соглашения). Понятно, что не все пользователи добросовестны и предпочтут злоупотребить правом для собственного развлечения — использовать фотоизображение третьего лица (знаменитости, людей из близкого окружения и др.), чтобы сгенерировать забавный видеоролик с его участием по заранее заданному описанию. Такие действия Пользователя будут нарушать Соглашение, и, согласно пп. 7.5 и 7.6 при получении Сервисом ПД Пользователь будет обязан предоставить Банку правовые основания их обработки, в том числе при подаче иска в отношении Банка, а также уведомить субъекта ПД о такой обработке в течение 3 рабочих дней.

¹⁸ Селюк А. С. Защита персональных данных в рамках использования технологий искусственного интеллекта // Аграрное и земельное право. 2025. № 4. URL: <https://cyberleninka.ru/article/n/zaschita-personalnyh-dannyh-v-ramkah-ispolzovaniya-tehnologiy-iskusstvennogo-intellekta> (дата обращения: 05.01.2026).

¹⁹ СЗ РФ. 2019. № 41. Ст. 5700.

²⁰ Литвин И. И. Особенности сбора, обработки и защиты персональных данных искусственным интеллектом // Вестник Уральского юридического института МВД России. 2021. № 4. URL: <https://cyberleninka.ru/article/n/osobennosti-sbora-obrabotki-i-zaschity-personalnyh-dannyh-iskusstvennym-intellektom> (дата обращения: 05.01.2026).

²¹ Пользовательское соглашение об использовании сервиса GigaChat // Портал для разработчиков SberDev. URL: <https://developers.sber.ru/docs/ru/policies/gigachat/agreement#7-personalnye-dannye> (дата обращения: 29.12.2025).

В рамках Соглашения, объем обрабатываемых Банком ПД Пользователя строго ограничивается информацией, предоставляемой им в ходе процедуры авторизации в Сервисе, при использовании Сервиса Партнера в рамках функциональных возможностей Сервиса и только в целях заключения и исполнения Соглашения, в том числе с целью использования Сервиса (п. 7.7). Такими условиями Банк пытается защитить себя от возможной ответственности за утечку ПД без согласия субъекта. Остаются не раскрытыми последствия непредставления правового основания обработки Пользователем. От этого зависит, будет ли обработка БПД прекращена, будут ли они обезличены или уничтожены или на них начнет распространяться общая Политика обработки персональных данных в ПАО Сбербанк²² (п. 7.8 Соглашения).

Обратимся к иностранному аналогу — китайскому DeepSeek. Согласно DeepSeek Privacy Policy²³ (далее — Политика) Сервис вправе обрабатывать ПД, которые Пользователь предоставляет. К таким данным относятся личные данные аккаунта, введенные при регистрации, текстовые и голосовые данные, подсказки, загруженные файлы, фотографии, отзывы, историю чатов и др. Обрабатываются ПД на основании перечня целей, среди которых выделяются, например создание учетных записей, обеспечение доступа и пользовательской коммуникации, совершенствование и развитие Сервисов путем анализа их использования и обучения алгоритмов машинного обучения и др. На основании вводных данных Сервис генерирует ответы по запросам Пользователей. При этом оператор в лице Hangzhou DeepSeek Artificial Intelligence Co., Ltd. отдельно оговаривает, что обязуется не извлекать или майнить информацию о голосовом фрагменте или распознавании лиц, или другие уникальные биологические характеристики, также используемые для идентификации конкретного человека, из голосовых данных или фотографий, которые были предоставлены Пользователем. Любопытно положение Политики в отношении общедоступных ПД: оператор вправе свободно их использовать из онлайн-источников и получать по согласию для обучения своих моделей и предоставления услуг. В то же время Пользователь всегда управомочен отказаться от использования ПД для обучения моделей или оптимизации технологий Сервиса. В данном контексте приведем позицию А. К. Жаровой, которая замечает, что использование общедоступных ПД для создания синтетического художественного произведения не может быть квалифицировано как правонарушение, если сам субъект сделал их общедоступными²⁴. Такое утверждение требует разъяснения. Если под «сам субъект делает персональные данные общедоступными» автор имел в виду обязательное предоставление согласия на обработку в соответствии с требованиями законодательства, то данное утверждение представляется верным. В противном случае, без какого-либо согласия ни одна технология генеративного ИИ не имеет права использовать БПД субъекта. Упоминается, что Сервис не предназначен для обработки конфиденциальных ПД (в частности, БПД), их не запрашивают, и Пользователи не должны предоставлять их Сервисам, как о себе, так и о других лицах. Оператор не занимается профилированием Пользователей и третьих лиц, но оговаривает возможность обработки ПД без согласия, только если это связано с исполнением юридических обязательств по запросам правоохранительных органов и требований законодательства.

Итак, соглашение сервиса GigaChat ПАО «Сбербанк» предусматривает запрет на ввод БПД, собственных и третьих лиц. Это направлено на предотвращение их неправомерной обработки и снижение рисков ответственности оператора. Политика DeepSeek также не ориентирована на обработку БПД, содержит предупреждение о

²² Политика обработки персональных данных в ПАО «Сбербанк» // URL: <https://www.sberbank.ru/privacy/policy> (дата обращения: 29.12.2025).

²³ DeepSeek Privacy Policy // URL: <https://cdn.deepseek.com/policies/en-US/deepseek-privacy-policy.html> (дата обращения: 29.12.2025).

²⁴ Жарова А. К. Технологии дипфейк: социально-правовые риски нарушения частной жизни лица и правовые решения // Правопорядок: история, теория, практика. 2025. № 2 (45). URL: <https://cyberleninka.ru/article/n/tehnologii-dipfeyk-sotsialno-pravovye-riski-narusheniya-chastnoy-zhizni-litsa-i-pravovye-resheniya> (дата обращения: 05.01.2026).

недопустимости их предоставления и исключает профилирование пользователей. Вместе с тем DeepSeek в отличие от российского сервиса прямо допускает возможность обработки БПД, ограничиваясь указанием на нежелательность передачи личной и конфиденциальной информации, без конкретизации формы и порядка получения согласия субъекта. Политики конфиденциальности обоих сервисов реализуются в рамках требований законодательства государств, на территории которых оказываются их услуги. При этом DeepSeek прямо предусматривает обработку ПД в целях обучения модели ИИ, при включении согласия субъекта на данную цель в общее согласие пользователя с пользовательским соглашением при начале использования сервиса. Такой подход не соответствует требованиям законодательства РФ, устанавливающего необходимость отдельного письменного согласия на обработку БПД согласно ч. 3 ст. 11 Федерального закона № 152-ФЗ.

4. ЕВРОПЕЙСКОЕ ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОБРАБОТКИ БПД В СИСТЕМАХ ГЕНЕРАТИВНОГО ИИ

Европейское законодательство устанавливает строгие правила обработки БПД в системах ИИ, классифицируя их как специальные категории данных с высоким риском. Основные нормы содержатся в GDPR и AI Act, которые запрещают или ограничивают противоправные практики обработки таких данных для защиты прав граждан. Биометрия требует явного согласия и пропорциональности использования. Так, нормативное содержание ст. 4 GDPR позволяет определить БПД как категорию данных, полученных в результате специальной технической обработки, в отношении физических, физиологических или поведенческих характеристик физического лица, идентифицирующие его. Например, это изображения лица или дактилоскопические данные. Обработка таких данных допускается только при наличии явного согласия субъекта в соответствии с заранее определенными целями либо в отдельных случаях, установленных статьей 9 GDPR.

Статья 5 AI Act посвящена методам использования ИИ, которые запрещены. Среди них п. (1)(f) и (g) выделяет именно запрет на использование и обработку БПД в ИИ. Так, режим запрета в отношении систем, осуществляющих категоризацию физических лиц на основе их БПД, исключает возможность их вывода на рынок и практического применения. Особый запрет направлен на недопустимость применения технологий распознавания эмоций на основе ИИ в контексте трудовой деятельности и образовательного процесса. Установленные ограничения не распространяются на обработку правомерно полученных биометрических данных (их маркировку и фильтрацию), а также на использование биометрической категоризации в правоохранительной деятельности. Запрет на анализ эмоций не применяется в случаях, когда соответствующая система ИИ используется или размещается на рынке для медицинских целей либо в целях обеспечения безопасности.

Всё это в совокупности с тем, что системы ИИ в области биометрической идентификации классифицируются как высокорисковые по ст. 6 и Annex III (п. 1) AI Act, включая удаленную идентификацию, категоризацию конфиденциальных атрибутов и характеристик, полученных в результате анализа и эмоциональное распознавание говорит о том, что в ЕС очень тщательно подходят к вопросу защиты прав граждан, касающихся обработки БПД. Для них обязательны: управление рисками, обеспечение качества данных, документация, прозрачность, надзор и кибербезопасность (ст. 9–15, 29 AI Act). Провайдеры обязаны проводить оценку соответствия и регистрировать высокорисковые системы ИИ в базу данных (ст. 49) и обеспечивать их прослеживаемость. AI Act не затрагивает GDPR, оставляя письменное согласие по ст. 4(11) GDPR за рамками своих норм — оно применимо только к безрисковым или разрешенным практикам в общем контексте защиты ПД.

Таким образом, в ЕС сформирован императивный подход к регулированию обработки БПД в системах ИИ, отнесенных к высокорисковым. В соответствии

с GDPR их обработка допускается исключительно при наличии явно выраженного, добровольного и конкретного согласия субъекта и только в рамках заранее определенных и законных целей. Использование БПД для иных целей возможно лишь при установлении их совместимости с первоначальными целями обработки. В научной литературе, в частности И. П. Ковалёвым, отмечается формирование комплексного регулирования применения ИИ для идентификации личности и необходимость совершенствования национального законодательства во избежание неправомерного ограничения прав и свобод посредством технологически нейтральных и доступных механизмов²⁵. Общий запрет на использование БПД в системах ИИ рассматривается как базовая гарантия их правовой защиты.

5. ПРОБЛЕМЫ СОВРЕМЕННОГО ПРАВОВОГО РЕГУЛИРОВАНИЯ

В ходе анализа мы пришли к выводу, что современное правовое регулирование обработки БПД в РФ имеет, безусловно, сильные стороны, но в научной литературе неоднократно отмечалось, что есть аспекты, которые важно системно переработать и внести определенные коррективы.

Так, А. К. Жарова предлагает связать генеративные ИИ, в особенности дипфейк, определенными методами контроля и мониторинга за контентом, фиксируя специальную маркировку на любом ИИ²⁶. Более того, только в случае прохождения подтверждения личности появляется возможность генерировать и публиковать новый контент. Всё это делается для недопущения пропуска случайно сгенерированного анонимного контента. Предложение ученого представляется весьма актуальным в свете активного развития технологий ИИ, крупного оборота ПД в запросах систем генеративного ИИ и уязвимости категорий ПД как объектов правовой защиты в эпоху цифровой трансформации. Кроме того, подобный подход используется в ЕС и показывает устойчивость и эффективность правового регулирования. О. С. Болотаева и Н. А. Новокшонова предлагают использовать в отношении обработки БПД специальный режим по аналогии с режимом исключительных прав, поскольку категория БПД затрагивает личные и имущественные интересы субъекта²⁷. По мнению О. С. Болотаевой, такой режим обеспечивает механизм контроля и защиты, тогда распоряжение исключительным правом на БПД возможно посредством заключения лицензионного договора. Здесь, конечно, возникает вопрос относительно целесообразности такого правового режима исключительных прав в то время, как существует отдельный институт согласия на обработку ПД. К тому же, как мы неоднократно замечали, в отношении БПД предусмотрена строгая законодательная письменная форма согласия. О. С. Болотаева считает, что эти два режима могут сосуществовать

²⁵ Ковалёв И. П. Правовое регулирование защиты личных прав человека при использовании технологий искусственного интеллекта // Вестник Московского университета имени С.Ю. Витте. Серия 2, Юридические науки. 2024. № 1 (41). URL: <https://cyberleninka.ru/article/n/pravovoe-regulirovanie-zaschity-lichnyh-prav-cheloveka-pri-ispolzovanii-tehnologiy-iskusstvennogo-intellekta> (дата обращения: 03.01.2026).

²⁶ Жарова А. К. Технологии дипфейк: социально-правовые риски нарушения частной жизни лица и правовые решения // Правопорядок: история, теория, практика. 2025. № 2 (45). URL: <https://cyberleninka.ru/article/n/tehnologii-dipfeyk-sotsialno-pravovye-riski-narusheniya-chastnoy-zhizni-litsa-i-pravovye-resheniya> (дата обращения: 05.01.2026).

²⁷ Болотаева О. С. Биометрические персональные данные как средства индивидуализации физического лица // Право и государство: теория и практика. 2024. № 8 (236). URL: <https://cyberleninka.ru/article/n/biometricheskie-personalnye-dannye-kak-sredstva-individualizatsii-fizicheskogo-litsa> (дата обращения: 27.12.2025) ; Новокшонова Н. А. Цифровая идентификация гражданина: современные вызовы // Вестник Челябинского государственного университета. Серия «Право». 2025. № 2. URL: <https://cyberleninka.ru/article/n/tsifrovaya-identifikatsiya-grazhdanina-sovremennye-vyzovy> (дата обращения: 03.01.2026).

вместе, поскольку лицензионный договор и согласие на обработку будут заключаться в разных целях. В частности, согласие на обработку целесообразно для реализации публичных целей, биометрической аутентификации и для правоохранительных целей. Признаем, что концепция исключительных прав на БПД имеет под собой основания. Тем не менее, на наш взгляд, этот институт вступает в противоречие с действующим законодательством. Во-первых, согласие на обработку БПД не требуется для публичных целей, которые перечисляет автор. Во-вторых, несмотря на выделение в п. 5 ч. 1 ст. 6 Федерального закона № 152 такого правового основания обработки ПД, как договор, стороной которого является субъект ПД, требование о письменной форме согласия на обработку БПД таково, что оно дается отдельно, кроме случаев, когда такое согласие не требуется (ч. 2 ст. 11). Поэтому представить случаи, когда может заключаться лицензионный договор на использование БПД без заключения соответствующего согласия на обработку БПД в письменной форме, представляется затруднительным.

И. Н. Мосечкин и другие авторы подсвечивают возможное ужесточение юридической ответственности и включение в УК специального состава преступления, криминализирующего создание и распространение дипфейков, цифровых подделок при отсутствии информированного согласия лица, чьи БПД используются²⁸. Это предполагает выработку квалифицирующих и конституирующих признаков. Авторы выявляют также регуляторные, организационные проблемы в контроле сбора, обработки, хранения и доступа к БПД и полагают, что существующие нормы, например ст. 272 УК РФ, недостаточны²⁹.

ЗАКЛЮЧЕНИЕ

Таким образом, считаем необходимым обозначить пробелы в правовом регулировании обработки БПД в РФ с предложениями по их исправлению. Во-первых, не придается императивная сила запретов на использование БПД в запросах генеративного ИИ. В силу этого любой Пользователь легко нарушает этот запрет. Опцией решения этой проблемы можно считать закрепление в законодательстве прямого запрета на обработку БПД в системах ИИ и установление за его нарушение административной ответственности по аналогии с тем, как это сделано в AI Act. Другой опцией является обязывание владельцев генеративных ИИ разрабатывать соответствующие механизмы проверки подлинности согласий субъектов на обработку. Поскольку единственным препятствием на пути к правомерной обработке БПД по-прежнему остается непрозрачная система получения такого согласия. Пользователю предоставляется возможность загружать любые фото, видео и аудио материалы, в том числе с изображениями и голосами реальных людей без продуманного механизма проверки наличия правового основания на такую обработку оператором. Во-вторых, получение согласия на обработку БПД в целях обучения нейросети. По мнению автора, согласие на такую цель необходимо обязывать давать всегда отдельно, поскольку ее указание совместно с остальными целями препятствует праву распоряжаться своими данными и возможности использовать сервисы без такого согласия. Иначе операторы обуславливают доступ к своим ресурсам обязанностью предоставить БПД для целей обучения, что прямо запрещено ст. 11 Федерального закона № 152-ФЗ.

²⁸ Цит. по: Мосечкин И. Н. Дипфейк-технологии и биометрические данные: направления уголовно-правового регулирования // Вестник СПбГУ. Серия 14, Право. 2025. № 1. С. 95–110. URL: <https://cyberleninka.ru/article/n/dipfeyk-tehnologii-i-biometricheskie-dannye-napravleniya-ugolovno-pravovogo-regulirovaniya> (дата обращения: 03.01.2026).

²⁹ Желудков М. А., Алексеева А. П. Обеспечение защищенности биометрических персональных данных от использования в криминальных целях // Вестник Санкт-Петербургского университета МВД России. 2025. № 2 (106). С. 159–169. URL: <https://cyberleninka.ru/article/n/obespechenie-zaschischennosti-biometricheskih-personalnyh-dannyh-ot-ispolzovaniya-v-kriminalnyh-tselyah> (дата обращения: 03.01.2026).

Поэтому лицо должно иметь возможность отказаться от предоставления БПД для обработки в целях обучения нейросети, при этом не теряя возможности использовать сервис в личных целях.

БИБЛИОГРАФИЯ

1. Болотаева О. С. Биометрические персональные данные как средства индивидуализации физического лица // Право и государство: теория и практика. — 2024. — № 8 (236).
2. Добробаба М. Б. Понятие персональных данных: проблема правовой определенности // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2023. — № 2. — С. 42–52. — DOI: 10.17803/2311-5998.2023.102.2.042-052.
3. Жарова А. К. Технологии дипфейк: социально-правовые риски нарушения частной жизни лица и правовые решения // Правопорядок: история, теория, практика. — 2025. — № 2 (45).
4. Желудков М. А., Алексеева А. П. Обеспечение защищенности биометрических персональных данных от использования в криминальных целях // Вестник Санкт-Петербургского университета МВД России. — 2025. — № 2 (106). — С. 159–169.
5. Жужгина А. А., Соловьева Д. Д. Правовое регулирование синтеза человеческого голоса с помощью технологий искусственного интеллекта // Вестник ННГУ. — 2024. — № 5.
6. Ковалёв И. П. Правовое регулирование защиты личных прав человека при использовании технологий искусственного интеллекта // Вестник Московского университета имени С.Ю. Витте. Серия 2, Юридические науки. — 2024. — № 1 (41).
7. Кутейников Д. Л., Ижаев О. А., Алексеевич Л. В., Зенин С. С. Неприкосновенность частной жизни в условиях использования систем искусственного интеллекта для удаленной биометрической идентификации личности // Lex russica. — 2022. — Т. 75. — № 2. — С. 121–131.
8. Литвин И. И. Особенности сбора, обработки и защиты персональных данных искусственным интеллектом // Вестник Уральского юридического института МВД России. — 2021. — № 4.
9. Мосечкин И. Н. Дипфейк-технологии и биометрические данные: направления уголовно-правового регулирования // Вестник СПбГУ. Серия 14, Право. — 2025. — № 1. — С. 95–110.
10. Новокшонова Н. А. Цифровая идентификация гражданина: современные вызовы // Вестник Челябинского государственного университета. Серия «Право». — 2025. — № 2.
11. Платонова Н. И. Современный подход к пониманию персональных данных // Право и современные государства. — 2017. — № 5.
12. Селюк А. С. Защита персональных данных в рамках использования технологий искусственного интеллекта // Аграрное и земельное право. — 2025. — № 4.

REFERENCES

1. Bolotaeva OS. Biometric personal data as a means of individualization of an individual. *Law and State: Theory and Practice*. 2024;8(236). (In Russ.).
2. Dobrobaba MB. The concept of personal data: the problem of legal certainty. *Courier of Kutafin Moscow State Law University (MSAL)*. 2023;2:42-52. (In Russ.). DOI: 10.17803/2311-5998.2023.102.2.042-052.
3. Kovalev IP. Legal regulation of the protection of personal human rights when using artificial intelligence technologies. *Bulletin of the Moscow University named after S.Yu. Witte. Series 2, Legal Sciences*. 2024;1(41).
4. Kuteinikov DL, Izhaev OA, Alekseevich LV, Zenin SS. Privacy in the realm of Artificial Intelligence Systems Application for Remote Biometric Identification. *Lex russica*. 2022;75(2):121-131. (In Russ.).

5. Litvin II. Features of the collection, processing and protection of personal data by artificial intelligence. *Bulletin of the Ural law institute of the Ministry of the interior of Russia*. 2021;4. (In Russ.).
6. Mosechkin IN. Deepfake technologies and biometric data: areas of criminal law regulation. *Vestnik of Saint Petersburg University. Law*. 2025;1:95-110. (In Russ.).
7. Novokshonova NA. Digital identification of a citizen: modern challenges. *Bulletin Chelyabinsk State Univesity. Law*. 2025;2. (In Russ.).
8. Platonova NI. Modern approach to understanding personal data. *Law and Modern States*. 2017;5. (In Russ.).
9. Selyuk AS. Protection of personal data in the framework of the use of artificial intelligence technologies. *Agrarian and Land Law*. 2025;4. (In Russ.).
10. Zharova AK. Deepfake technologies: social and legal risks of violation of a person's privacy and legal decisions. *Law and Order: History, Theory, Practice*. 2025;2(45).
11. Zheludkov MA, Alekseeva AP. Ensuring the protection of biometric personal data from criminal use. *Vestnik of the St. Petersburg University of the Ministry of Internal Affairs of Russia*. 2025;2(106):159-169. (In Russ.).
12. Zhuzhgina AA, Solovyova DD. Legal regulation of the synthesis of human voice using artificial intelligence technologies. *Vestnik of Lobachevsky University of Nizhni Novgorod*. 2024;5. (In Russ.).