

DOI: 10.17803/1729-5920.2025.227.10.090-106

С. С. КузнецоваУральский государственный юридический
университет имени В.Ф. Яковлева
г. Екатеринбург, Российская Федерация

Особенности правового регулирования скоринга в Соединенных Штатах Америки и Европейском Союзе

Резюме. В работе проведен анализ правового регулирования скоринговых моделей в США и ЕС. Рассмотрены отдельные вопросы рейтингования личности с применением автоматизированных систем: источники информации и предъявляемые к ней требования, основания обработки данных, прозрачность скоринговых моделей; осуществлена оценка законодательства о регулировании систем искусственного интеллекта с позиции его эффективности в обеспечении защиты прав человека. Уделяется внимание вопросу недобросовестной практики обработки данных, в том числе с применением скоринговых моделей, брокерами данных в США, что обусловлено неэффективным, «лоскутным» подходом к правовому регулированию. Сделан вывод о том, что в цифровом пространстве согласие на обработку персональных данных, в том числе специальное — для использования полностью автоматизированных систем, утратило ценность и американский подход по предоставлению права на отказ от автоматизированной обработки предпочтителен. Обоснована особая значимость правового отражения принципов достоверности и полноты информации, положенной в основу скоринговой модели, а также оценки качества данных, используемых для разработки системы искусственного интеллекта. Сделан вывод о недостаточной правовой разработанности в европейском законодательстве обязанностей оператора системы искусственного интеллекта по обеспечению непредвзятости при работе с системой. Автор обращается к отдельным проблемам цифрового скоринга, т.е. рейтингования личности с использованием цифровых следов. На основании правоприменительной практики определен объем информации, подлежащей раскрытию в связи с применением скоринговых моделей, в том числе производных данных.

Ключевые слова: скоринг; цифровой скоринг; цифровые следы; искусственный интеллект; автоматизированное принятие решений; персональные данные; предвзятость системы принятия решений; производные данные

Для цитирования: Кузнецова С. С. Особенности правового регулирования скоринга в Соединенных Штатах Америки и Европейском Союзе. *Lex russica*. 2025. Т. 78. № 10. С. 90–106. DOI: 10.17803/1729-5920.2025.227.10.090-106

Благодарности. Исследование выполнено при финансовой поддержке РНФ в рамках научного проекта 24-28-01378 «Разработка концепции правового регулирования цифрового профилирования, социального скоринга и использования «цифровых следов»».

Features of Legal Regulation of Scoring in the United States of America and the European Union

Svetlana S. KuznetsovaUral State Law University named after V.F. Yakovlev
Ekaterinburg, Russian Federation

Abstract. The paper analyzes the legal regulation of scoring models in the USA and the EU. It examines specific issues of personal rating using automated systems: information sources and requirements for it, legal grounds for

© Кузнецова С. С., 2025

data processing, transparency of scoring models; legislation on the regulation of artificial intelligence systems is evaluated from the perspective of its effectiveness in ensuring the protection of human rights. Attention is being paid to the issue of unfair data processing practices, including the use of scoring models by data brokers in the United States, which is caused by an ineffective «patchwork» approach to legal regulation. It is concluded that in the digital space consent to the processing of personal data, including the allocation of a special one for the use of fully automated systems, has lost its value and the American approach to granting the right to refuse automated processing is preferable. The author substantiates the special importance of the legal reflection of the principles of reliability and completeness of the information underlying the scoring model, as well as the assessment of the quality of data used to develop an artificial intelligence system. The conclusion is made about the insufficient legal elaboration in the European legislation of the duties of the operator of the artificial intelligence system to ensure impartiality when working with the system. The author addresses specific problems of digital scoring, i.e., personal rating using digital footprints. Based on law enforcement practice, the amount of information to be disclosed in connection with the use of scoring models, including derived data, has been determined.

Keywords: scoring; digital scoring; digital footprints; artificial intelligence; automated decision-making; personal data; decision-making system bias; derived data

Cite as: Kuznetsova SS. Features of Legal Regulation of Scoring in the United States of America and the European Union. *Lex Russica*. 2025;78(10):90-106. (In Russ.). DOI: 10.17803/1729-5920.2025.227.10.090-106

Acknowledgements. The research was supported by the Russian Science Foundation, project No. 24-28-01378 titled «Development of the concept of legal regulation of digital profiling, social scoring and the use of «digital footprints».

Введение

Понятие скоринга впервые стало широко использоваться в мире в связи с деятельностью кредитных организаций, когда в 1989 г. американской фирмой FICO (Fair Isaac Corporation) банковскому сообществу была предложена модель кредитного скоринга как «технология математического и статистического методов оценки уровня кредитного риска, связанного с конкретным заемщиком»¹. Сфера применения скоринга постепенно расширялась за счет внедрения в деятельность страховых организаций, компаний, оказывающих услуги связи, в научную деятельность и медицину², ее применения для оценки потенциальных работников в процессе трудоустройства, при сдаче в аренду жилья и т.д. Также скоринговая система интегрирована в деятельность органов государ-

ственной власти отдельных зарубежных стран с целью оценки соответствия физических лиц требованиям, предъявляемым для получения последними социальной помощи и услуг³, а в Китайской Народной Республике для оценки поведения юридических лиц и граждан с позиции соблюдения законодательства государства⁴.

На сегодняшний день стремительное развитие скоринговых моделей связано с появлением технологий, которые позволяют осуществлять цифровой скоринг личности, — Big Data, Data Mining, искусственный интеллект и т.д. Первые две технологии позволили получить доступ к информации, хранимой в цифровом пространстве, к так называемым цифровым следам пользователя Интернета, которые, в отличие от физических следов, «не стираются со временем, не исчезают и доступны для потенциально неограниченного круга других участ-

¹ Агафонова В. В., Вишневер В. Я., Фрумусаки С. В. Технологическая эволюция кредитного скоринга в системе банковского потребительского кредитования // Вестник Волжского университета имени В.Н. Таищева. 2018. Т. 2. № 3. С. 22.

² Desai N., Gross J. Scoring systems in the critically ill: uses, cautions, and future directions // BJA Education. 2019. No. 19 (7). P. 212–218. DOI: 10.1016/j.bjae.2019.03.002.

³ Germundsson N., Stranz H. Automating social assistance: Exploring the use of robotic process automation in the Swedish personal social services // International Journal of Social Welfare. 2023. No. 33 (17). P. 1–12. DOI: 10.1111/ijsw.12633.

⁴ Рувинский Р. З. Правовые аспекты внедрения системы социального кредита в современное публичное управление. Н. Новгород : НИУ РАНХиГС, 2022. С. 68–69.

ников интернет-коммуникации»⁵. Технология искусственного интеллекта ускорила процесс принятия решений по формированию рейтинга, а также решений, основанных на оценке рейтинга юридического или физического лица. Обработка цифровых следов в целях оценки кредитоспособности заемщика и риска его дефолта позволила расширить линейку банковских кредитных услуг. Так, например, внедрение платежной системы Ху бей торговой онлайн-платформы «Алибаба» увеличило число продаж за счет предоставления краткосрочных кредитов и рассрочек тем лицам, которые не имеют кредитной истории: «Традиционные банки не выдают деньги физическим лицам, потому что у них нет надежного кредитного рейтинга. Фактически большинство китайцев, по западным стандартам, просто “не поддаются оценке”: только у 25 % населения есть кредитная история»⁶. Таким образом, цифровой скоринг представляет собой процесс оценки субъекта данных на основе обработки альтернативных источников информации о нем — цифровых следов.

Проблематика использования цифровых следов в моделях скоринга вызывает большой интерес; многие исследователи отмечают, что «нетрадиционная» скоринговая система, основанная на использовании информации, полученной из онлайн-пространства, эффективно решает задачи бизнеса по привлечению новых клиентов; при этом результаты оценки цифровых следов позволяют представить информацию о кредитоспособности заемщика, не уступающую, а иногда и превышающую по точности

ту, которая формируется в рамках традиционной скоринговой модели⁷. Несмотря на то что цифровые скоринговые модели рассматриваются на сегодняшний день преимущественно с позиции открывающихся благодаря им новых возможностей рынка⁸, важно оценивать и те риски, которые они несут. Во-первых, обработка большого объема цифровых следов человека по своей сути является вмешательством в частную жизнь. В современном мире избежать такого вмешательства невозможно, но поиск баланса интересов личности, с одной стороны, и субъектов предпринимательской деятельности или органов публичной власти, осуществляющих обработку цифровых следов, — с другой, необходим, поскольку в ином случае право на неприкосновенность частной жизни в цифровом пространстве просто исчезнет.

Во-вторых, совершенствование систем искусственного интеллекта стимулирует их внедрение в различные сферы жизни человека и общества; более простые автоматизированные системы принятия решения, основанные на правилах и логике, разработанных специалистами, вытесняются генеративными моделями принятия решений, которые обучаются на огромных наборах данных; их возможности приобретают признаки универсализма — исчезает необходимость программирования для конкретной задачи. Как справедливо отмечается в Регламенте Европейского Союза «Об искусственном интеллекте»⁹, системы искусственного интеллекта оказывают воздействие на реализацию широкого круга прав, в том числе права на уважение достоинства лично-

⁵ Мочалов А. Н. Парадокс анонимности в Интернете и проблемы его правового регулирования // Вестник СурГУ. 2021. № 4 (34). С. 116.

⁶ Chinese Fintechs Use Big Data to Give Credit Scores to the ‘Unscorable’ // URL: <https://www.forbes.com/sites/rebeccafeng/2017/07/25/chinese-fintechs-use-big-data-to-give-credit-scores-to-the-unscorable/#45b0e6ed410a> (дата обращения: 01.04.2025).

⁷ Berg T., Burg V., Gombović A., Puri M. On the Rise of FinTechs — Credit Scoring Using Digital Footprints // The Review of Financial Studies. 2020. No. 7. P. 2847 ; Fuster A., Plosser M., Schnabl Ph., Vickery J. The Role of Technology in Mortgage Lending. Federal Reserve Bank of New York Staff Reports, No. 836. February 2018 // URL: https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr836.pdf (дата обращения: 01.04.2025). P. 19.

⁸ Луняков О. В., Лунякова Н. А. Развитие каналов кредитования в условиях перехода к цифровой экономике: моделирование спроса // Финансы: теория и практика. 2018. № 22 (5). С. 79. DOI: 10.26794/2587-5671-2018-22-5-76-89.

⁹ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No. 300/2008 (EU) No. 167/2013, (EU) No. 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) // URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> (дата обращения: 21.03.2025).

сти, неприкосновенность частной и семейной жизни, защиту персональных данных, свободу выражения мнений и информации, свободу собраний и объединений, права на образование, прав потребителей, трудящихся, лиц с ограниченными возможностями, права интеллектуальной собственности, права на эффективную защиту и справедливое судебное разбирательство, права на надлежащее управление, а также могут создавать дискриминационные факторы при реализации субъективных прав. Соответственно, вопросы применения систем полностью автоматизированного принятия решений в отношении человека предполагают необходимость разработки высоких стандартов стабильности и безопасности таких систем, а также определения условий их применения и установления ограничений по применению в наиболее уязвимых для человека сферах.

Целью данного исследования является выявление и формулирование основных подходов к правовому регулированию скоринга личности, в том числе с применением цифровых следов, в законодательстве зарубежных стран с позиции обеспечения баланса интересов субъекта данных и обработчика информации. В качестве объекта исследования выбрано законодательство Соединенных Штатов Америки и стран Европейского Союза, что обусловлено следующими факторами: США являются мировым лидером в сфере искусственного интеллекта¹⁰; вместе с тем именно в рамках Европейского Союза был принят первый в мире комплексный акт, направленный на урегулирование вопроса применения систем искусственного интеллекта в отношении человека.

Правовые основы применения скоринга

Правовое регулирование скоринга личности в США осуществляется как на федеральном уровне, так и на уровне штатов. На федеральном уровне регулируются кредитное профилирование и скоринг потребителя специальными субъектами — агентствами по кредитной отчетности и федеральными органами государственной

власти. Основные принципы и правила обработки личной информации при осуществлении кредитного профилирования и скоринга сформулированы в федеральных законах «О добросовестной кредитной отчетности»¹¹ и «О равных возможностях получения кредита»¹².

Законодательство штатов о личной информации будет использоваться в следующих случаях: а) сбор и обработка информации о личности поставщиками информации; б) сбор, обработка информации и формирование скоринговых моделей операторами данных, которые не являются агентствами по кредитной отчетности; в) обработка данных о личности и формирование скоринговых чисел органами публичной власти штатов в процессе реализации государственных полномочий. На сегодняшний день законодательство о защите личной информации принято в 20 штатах США; в ряде штатов (Индиана, Кентукки, Мэриленд, Род-Айленд) соответствующие законы еще не вступили в действие. Региональное законодательство не распространяется на всех операторов обработки личной информации резидентов штатов — оно ориентированно преимущественно на крупных операторов: в штатах Индиана, Кентукки к таким операторам относятся те, кто ежегодно обрабатывает информацию не менее чем о 100 000 жителей штата или 25 000 при условии получения не менее половины прибыли организации от продажи данных, в штате Миннесота — не менее четверти прибыли. В штатах Нью-Гемпшир и Мэриленд под действие рассматриваемых законов попадают те организации, которые обрабатывают данные не менее чем о 35 000 жителей ежегодно с сокращением до 10 000 при условии получения не менее четверти доходов от продажи данных. В штате Калифорния соответствующий закон распространяется лишь на те организации, которые отвечают одному из следующих требований: ежегодно делятся, продают или покупают информацию о 100 000 и более потребителей; 50 % дохода получают от данной деятельности, или их ежегодный общий доход составляет более 25 млн долл. в год. Таким образом, законодательство позволяет небольшим

¹⁰ Global AI Power Rankings: Stanford HAI Tool Ranks 36 Countries in AI // URL: <https://hai.stanford.edu/news/global-ai-power-rankings-stanford-hai-tool-ranks-36-countries-in-ai> (дата обращения: 21.04.2025).

¹¹ Fair Credit Reporting Act, 1970. 15 U.S.C § 1681 // URL: https://www.ftc.gov/system/files/ftc_gov/pdf/fcra-may2023-508.pdf (дата обращения: 01.04.2025).

¹² Equal Credit Opportunity Act, 1974. 15 U.S.C. § 1691 // URL: <https://www.ftc.gov/legal-library/browse/statutes/equal-credit-opportunity-act> (дата обращения: 01.04.2025).

организациям осуществлять обработку данных без соблюдения установленных им требований. Соответственно, персональные данные жителей большей части страны не получают должную защиту в случаях, где в отношении них используются системы автоматизированного принятия решений, не подпадающие под действие федерального законодательства.

В Европейском Союзе действуют общеобязательные для стран-членов регламенты — Общий регламент по защите данных¹³, в котором определены правила и требования их обработки вне зависимости от сферы деятельности контролера, а также Регламент «Об искусственном интеллекте», определяющий условия и порядок использования систем искусственного интеллекта общего назначения, в том числе для принятия решений в отношении личности, т.е. для профилирования и скоринговых моделей. В отличие от американского законодательства, круг субъектов, на которых распространяется действие европейских актов, не ограничен их основным видом деятельности или объемом их доходов / персональных данных, которые они обрабатывают; важным является тот факт, что они в процессе своей деятельности осуществляют обработку персональных данных (контролеры данных) или разрабатывают, размещают на рынке, используют либо вводят в эксплуатацию систему искусственного интеллекта общего назначения (поставщики, операторы). Таким образом, наблюдается универсализация актов, упрощается понимание человеком условий их применения.

В национальном законодательстве стран — членов ЕС также приняты и действуют законы о защите персональных данных, которые имплементируют в национальное законодательство положения Общего регламента; при этом он предусматривает право стран самостоятельно урегулировать отдельные вопросы (например, определить основания применения полностью автоматизированных систем принятия

решений, когда не требуется получения согласия субъекта данных). Регламент «Об искусственном интеллекте» тоже предусматривает право стран ЕС установить дополнительные гарантии защиты прав человека в процессе применения в отношении него систем искусственного интеллекта (например, ввести или сохранить более строгие правила для защиты прав работников, а также при использовании систем дистанционной идентификации личности, самостоятельно определить порядок реализации норм названного Регламента, в том числе проведения аудитов, наложения штрафных санкций). Государства-члены не могут осуществлять правовое регулирование, направленное на предоставление права на использование запрещенных систем социального скоринга или снижение требований к высокорисковым системам, к которым относится большинство скоринговых систем.

В США акт, аналогичный европейскому Регламенту «Об искусственном интеллекте», отсутствует. В 2023 г. Дж. Байденом был подписан Указ «О безопасных, надежных и заслуживающих доверия разработке и использовании искусственного интеллекта»¹⁴, который определял некоторые меры, направленные на защиту прав человека в условиях применения к нему автоматизированных систем принятия решений. Например, были предусмотрены создание единых стандартов разработки и развертывания безопасных систем, аудит применения автоматизированных систем в уголовном процессе и в деятельности органов публичной власти для определения соответствия лица требованиям, предъявляемым для получения мер государственной поддержки, сформулирована задача определить сферы, в которых применение искусственного интеллекта с целью принятия значимых решений в отношении человека должно быть запрещено. Однако в 2025 г. Президент США Д. Трамп издал Указ «Об устранении препятствий к американскому лидерству в сфере искусственного интеллекта»¹⁵,

¹³ 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> (дата обращения: 01.04.2025).

¹⁴ Executive Order 14110, 2023 (Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence) // URL: <https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence> (дата обращения: 12.04.2025).

¹⁵ Executive Order 14179, 2025 (Removing Barriers to American Leadership in Artificial Intelligence) // URL: <https://www.federalregister.gov/documents/2025/01/31/2025-02172/removing-barriers-to-american-leadership-in-artificial-intelligence> (дата обращения: 12.04.2025).

направленный на отмену Указа 2023 г. и всех актов, которые были приняты в его исполнение и «могут быть препятствием» для достижения поставленной цели. Таким образом, все попытки сформировать концепцию безопасных систем искусственного интеллекта на сегодняшний день провалились.

Правовые гарантии реализации прав человека в процессе сбора информации в целях скоринга

Онлайн-пространство предоставляет широкие возможности по обработке самых разнообразных цифровых следов. RiskSeal заявляет, что при формировании скоринговой модели, основанной на цифровых следах, значение могут иметь данные сервисов «Купи сейчас, заплати позже», демографические и геоданные, привычки и статистика просмотров, почтовый адрес, а также данные о подписках¹⁶. Бертран и Каменица отмечают, что большое значение имеет и устройство, с которого осуществляется выход в онлайн-пространство: наличие iOS на устройстве является одним из лучших предсказателей финансовой стабильности лица¹⁷. Кроме того, использованию цифровых следов способствует признание законным скрейпинга¹⁸, который позволяет не только выделить всех пользователей, но и их «индивидуальные характеристики»¹⁹. Аналитики отмечают, что в 2023 г. 62 % финансовых институтов использовали альтернативные данные в целях профилирования, скоринга и андеррайтинга заемщиков²⁰. Поэтому вопрос о требованиях к порядку сбора и «качеству» информации, которая будет положена в основу скоринга, имеет одно из определяющих значений в борьбе с дискриминацией.

Федеральный закон США «О добросовестной кредитной отчетности» в качестве субъектов формирования кредитного скоринга определяет «агентство по отчетности потребителей» и «агентство по предоставлению информации

о потребителях, которое собирает и хранит файлы о потребителях на общенациональной основе» (далее — национальное агентство), таким образом, распространяя свое действие в первую очередь на указанных субъектов. Задачей любого агентства по отчетности являются сбор и обработка информации о человеке с целью формирования его кредитного профиля и скорингового числа, а также передача этой информации третьим лицам в порядке, предусмотренном законодательством. Принципиальным отличием национальных агентств от агентств по отчетности потребителей является то, какой объем личной информации и из каких источников данные операторы получают. Национальные агентства формируют отчеты преимущественно на основании традиционных источников: общедоступных записей (записей, созданных органами исполнительной власти в рамках их деятельности), а также данных, полученных от физических лиц и организаций, которые предоставляют такую информацию в рамках своей основной деятельности (кредитных и страховых организаций). Иные агентства по отчетности потребителей могут заниматься сбором и обработкой информации с целью профилирования личности и скоринга для отдельных узкоспециализированных целей: рекрутинговых и страховых компаний, организаций, предоставляющих различные виды услуг (услуги мобильной связи, Интернета), арендодателей и т.д.). Таким образом, они заинтересованы в сборе и обработке информации, которая позволяет сформировать уникальный продукт, в связи с чем обработка «альтернативных данных», в том числе цифровых следов, приобретает популярность.

Федеральное законодательство не устанавливает специальных требований к источникам сбора информации, однако во избежание формирования дискриминационных скоринговых чисел требует того, чтобы информация, содержащаяся в отчете о потребителе, была

¹⁶ The Top 10 Credit Scoring Trends That Will Reshape the Future of Lending // URL: <https://riskseal.io/blog/top-10-digital-credit-scoring-trends> (дата обращения: 01.03.2025).

¹⁷ Bertrand M., Kamenica E. Coming apart? Lives of the rich and poor over time in the United States. Chicago, 2017.

¹⁸ LinkedIn Corporation v. HiQ Labs Inc., No. 17-16783 (9th Cir. 2022).

¹⁹ Вилкова О. В. К вопросу о научной осмысленности применения веб-скрейпинга как метода сбора данных в социологических исследованиях // Вестник Томского государственного университета. Философия. Социология. Политология. 2020. № 54. С. 165. DOI: 10.17223/1998863X/54/16.

²⁰ Alternative credit data 101: What it is and what it's used for // URL: <https://stripe.com/resources/more/alternative-credit-data-101-what-it-is-and-what-its-used-for> (дата обращения: 01.03.2025).

достоверной и полной. Обязанность оценивать достоверность и полноту информации в первую очередь возлагается на поставщиков данных. Они должны воздерживаться от передачи информации, если есть «разумные основания предполагать» ее неточность, а также если потребитель заявил об ошибках. Поставщики должны определять условия и порядок открытия прямого спора с потребителем. Агентства, в свою очередь, обязаны принимать разумные действия для обеспечения конфиденциальности, точности, релевантности и надлежащего использования информации, проверять наличие у поставщика положения о порядке открытия спора, рассматривать в установленные законом сроки заявления потребителя о наличии неполной или недостоверной информации и в случае подтверждения данного факта удалять ее.

Региональное законодательство также не ограничивает источники сбора данных о субъекте, но при этом, в отличие от федерального законодательства, не содержит принципа точности и полноты информации. Любые корректировки осуществляются в процессе реализации права субъекта данных требовать внесения в информацию изменений. а в штате Айова право на корректировку не предусмотрено в принципе. Эффективность скоринговых моделей напрямую зависит от полноты и достоверности данных, положенных в основу формирования рейтинга и скоринговых чисел, поэтому презумпция достоверности информации создает угрозу нарушения прав человека. В США ввиду того, что законодательство не требует получения согласия на продажу персональных данных, профилирование и рейтингование личности является направлением деятельности большого числа организаций. Субъект данных попросту не в состоянии отследить все факты обработки информации о нем. В результате о наличии недостоверной информации, положенной в основу автоматизированного принятия решения, человек узнает уже после того, как негативное для него решение было принято.

В США необходимо разграничивать агентства по отчетности потребителей и так называемых брокеров данных. Федеральное зако-

нодательство не раскрывает понятие «брокер данных», однако в отдельных штатах их статус определен. В Калифорнии под брокерами данных понимаются организации, «которые сознательно собирают и продают третьим лицам личную информацию о потребителе, с которым компания не имеет прямых отношений»²¹. В данное понятие не включаются организации, подпадающие под действие федерального законодательства. Как и агентства по отчетности потребителей, брокеры данных занимаются аккумулярованием значимой для конечного пользователя информации о личности, формированием профилей и скорингом, однако деятельность агентства по отчетности связана с формированием кредитных отчетов, которые предоставляются только для определенных в законе целей (кредита или страхования, личных, семейных или бытовых целей, трудоустройства и т.д.), в то время как брокеры формируют и передают третьим лицам профили и скоринговые числа в целях, не определенных в законе. Таким образом, брокеры могут собирать информацию о личности из различных источников, в том числе путем обработки цифровых следов, формировать производные данные и скоринговые числа, продавать информацию заинтересованным субъектам, но никакие гарантии федерального законодательства на них не распространяются. В конце 2024 г. на обсуждение был внесен проект правил «О защите американцев от вредоносных практик брокеров данных»²², который предусматривает распространение положений федерального закона на брокеров в случае, если они передают информацию о кредитной истории потребителя, кредитном рейтинге, доходе или финансовом уровне, вне зависимости от целей использования данной информации или в случае, если любая переданная брокерами третьим лицам информация будет использоваться для целей, предусмотренных Федеральным законом «О добросовестной кредитной отчетности». На сегодняшний день названный проект правил по-прежнему находится на этапе обсуждений.

Брокеры данных рассматриваются как серьезная угроза правам человека, демократическим институтам и национальной безопасности

²¹ California Delete Act. SB. 362, 2023.

²² Protecting Americans From Harmful Data Broker Practices (Regulation V), Consumer Financial Protection Bureau 12 CFR Part 102 [Docket No. CFPB-2024-0044] RIN 3170-AB27 // URL: <https://www.federalregister.gov/documents/2024/12/13/2024-28690/protecting-americans-from-harmful-data-broker-practices-regulation-v> (дата обращения: 07.04.2025).

США. Дж. Шерман отмечает, что «федеральные агентства США — от Федерального бюро расследований (ФБР) до Иммиграционной службы США и Таможенной службы — покупают данные у брокеров — без ордеров, общедоступного раскрытия информации или строгого надзора — для выполнения своих полномочий — от уголовных расследований до депортации. При этом компании — брокеры данных обходят ограничения, налагаемые на иные компании, связанные с правом последних напрямую передавать данные правоохранительным органам. Федеральные правительственные агентства, использующие данные, также обходят различные правовые ограничения, действующие в отношении обысков и изъятий...»²³

Пробелы в федеральном регулировании частично восполняются законодательством штатов. В штате Калифорния на брокеров данных возложена обязанность регистрироваться для осуществления обработки личной информации о жителях штата в целях дальнейшей продажи. Такая регистрация предусматривает выполнение ряда правил, в том числе подтверждение факта соблюдения Закона «О защите личной информации потребителей»²⁴ штата Калифорния, а также удаление информации по требованию субъекта данных.

В рамках ЕС действует концепция необходимости получения согласия на обработку персональных данных, а в отношении их сбора устанавливаются требования точности, полноты, целевого использования. Кроме того, в отличие от Соединенных Штатов, в странах ЕС отсутствует презумпция возможности продажи персональных данных третьим лицам; для этого требуется получение согласия субъекта данных.

Правовые основания и условия применения скоринговых моделей

Федеральный закон США «О добросовестной кредитной отчетности» не предусматривает необходимость получения от потребителя согласия на использование в отношении него пол-

ностью автоматизированных систем принятия решения, так же как и возражать против применения скоринговых моделей, поскольку презюмируется заинтересованность всех субъектов правоотношений в рейтинговании личности. Краеугольным принципом Закона «О равных возможностях кредитования» является запрет дискриминации по признакам расы, цвета кожи, религии, национального происхождения, пола, семейного положения, возраста, а также по причине того, что заемщик получает меры государственной поддержки. Очевидно, что по общему правилу соответствующая информация не может быть положена в основу автоматизированной системы принятия решений, однако в отдельных случаях законодательство такую возможность предусматривает: когда проверка возраста и семейного положения необходима для оценки прав субъекта данных на получение конкретного кредита или мер защиты без определения общего показателя кредитоспособности, факт получения государственной поддержки используется для оценки оснований продолжения ее предоставления и т.д.

Несмотря на попытки государства гарантировать недискриминационное рейтингование личности, в условиях многообразия кредитных профилей, скоринговых моделей и чисел дискриминационная уязвимость человека возрастает, так как в различных скоринговых моделях по-разному могут учитываться те или иные факты биографии лица²⁵. Как справедливо отмечает Нэйт Ван Дузер, «выбор исходных данных, которые следует учитывать при расчете кредитного рейтинга, может иметь разное влияние. Например, вы можете получить лучшую кредитную историю, регулярно выплачивая ипотеку, но нерегулярно выплачивая арендную плату. Такое необоснованное предпочтение при выплате ипотеки непропорционально сильно сказывается на чернокожих и испаноязычных потребителях, которые долгое время были исключены из рынков жилья и в результате имеют гораздо более низкие показатели владения жильем. В свою очередь более низкие кредитные рейтинги затрудняют для чернокожих и испаноязычных

²³ *Sherman J.* Data Brokers and Sensitive Data on U. S. Individuals: Threats to American Civil Rights, National Security, and Democracy. 2021 // URL: <https://techpolicy.sanford.duke.edu/wp-content/uploads/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf> (дата обращения: 07.04.2025). P. 9.

²⁴ California Consumer Privacy Act, 2018.

²⁵ *Rice L., Swesnik D.* Discriminatory Effects of Credit Scoring on Communities of Color. National Fair Housing Alliance, 2012. URL: <https://nationalfairhousing.org/wp-content/uploads/2017/04/NFHA-credit-scoring-paper-for-Suffolk-NCLC-symposium-submitted-to-Suffolk-Law.pdf> (дата обращения: 15.04.2025).

людей возможность стать владельцами жилья, что снижает их кредитные рейтинги и увековечивает цикл неравенства»²⁶. Таким образом, исключение из скоринговой модели, например, информации о расе потребителя не предотвращает того, что использование иных критериев оценки приведет к расовой дискриминации. Поэтому борьба с предвзятостью систем скоринга обеспечивается иными способами, например обеспечением прозрачности формирования скорингового числа (рейтинга), а также гарантированием права обжаловать его, если его применение привело к дискриминации.

В законодательстве штатов предусмотрено право на получение информации об использовании систем автоматизированного принятия решений, а также право отказаться от их применения, если это ведет «к юридическим или иным значимым последствиям». В штатах Калифорния, Колорадо²⁷ понятие решений, имеющих существенные последствия, раскрыто: к ним относятся случаи предоставления или отказа в предоставлении финансовых, кредитных услуг, услуг страхования, жилья, зачисления в образовательное учреждение, уголовное правосудие (например, внесение залоговых обязательств), трудоустройство или возможность заключения контрактов, получение компенсации, медицинских услуг или основных товаров или услуг (например, продуктов, лекарств, средств гигиены или топлива), а также получение государственных услуг (в штате Колорадо).

В Общем регламенте по защите данных ЕС установлен запрет на применение полностью автоматизированных систем принятия решения, в том числе скоринга, в случае, если это ведет к юридическим или аналогичным значимым последствиям. Данный запрет не является абсолютным и предполагает исключения: его применение возможно с согласия субъекта данных или в случае, когда это необходимо для заключения или исполнения договора. Также алгоритм полностью автоматизированного при-

нятия решения может быть разрешен законодательством государств Европейского Союза при обеспечении последними защиты прав субъекта данных.

Актуальным вопросом применения автоматизированных систем принятия решений является реальность и эффективность практики получения согласия субъекта данных. В статье 4 названного Регламента сформулированы основные требования к согласию: свободное, конкретное, осознанное, однозначно идентифицирующее намерение субъекта данных. Однако в онлайн-пространстве получение согласия, соответствующего указанным требованиям, представляет большую сложность.

Во-первых, несмотря на то что в практике ЕС делается акцент на простоте и доступности языка информирования об условиях и порядке обработки данных, о необходимости получения самостоятельного согласия на применение полностью автоматизированных систем обработки данных, многие исследователи скептически относятся к концепции согласия в целом, отмечая излишнюю сложность используемой при этом юридической терминологии, которая не позволяет реально понимать условия обработки данных²⁸. Поведение человека в онлайн-пространстве значительно отличается от его поведения в обычной жизни, Интернет рассматривается как средство ускорения выполнения поставленных задач, а «качественные результаты показывают, что участники считают политику помехой и игнорируют ее ради достижения целей цифрового производства, не сдерживаясь средствами ее достижения»²⁹. В случае если речь идет о предоставлении права на использование полностью автоматизированных систем принятия решений, ввиду того, что человек нередко не осознает возможности алгоритмов по формированию новой значимой информации, в том числе производных данных, а также того, что формирование производных данных определяется только как потенциальная возмож-

²⁶ Duzer N. V. The Discriminatory Impact of Credit Scores. April 4, 2023 // URL: <https://www.publicjustice.net/the-discriminatory-impact-of-credit-scores/> (дата обращения: 15.04.2025).

²⁷ Colorado Consumer Protection Act, § 6-1-101–115 C.R.S.

²⁸ Martin K. Privacy Notices as Tabula Rasa: An Empirical Investigation into How Complying with a Privacy Notice is Related to Meeting Privacy Expectations Online // Journal of Public Policy & Marketing. 2015. Vol. 34 (2). P. 70. DOI: 10.1509/jppm.14.139 ; Abrusio J. The (In)Efficacy of Consent for the Processing of Personal Data // Global Network Journal. 2024. No. 6 (1). P. 199–200.

²⁹ Obar J. A., Oeldorf-Hirsch A. The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services // Information, Communication & Society. 2018. No. 23 (1). P. 128. DOI: 10.1080/1369118X.2018.1486870.

ность, уровень озабоченности субъекта данных по-прежнему остается низким.

Во-вторых, в онлайн-пространстве широко распространены модели, когда субъекту данных предлагаются два варианта поведения: оплатить услугу или получить ее бесплатно в обмен на предоставление согласия на обработку персональных данных, в том числе с применением полностью автоматизированных систем. Как отмечается в разъяснениях Европейского совета по защите данных, предложение исключительно платной альтернативы услуге не позволяет соблюсти требование свободного согласия, поэтому в случае, если контролер принимает решение о предоставлении бесплатных услуг при условии согласия на обработку персональных данных для целей поведенческой рекламы, он должен обязательно предусмотреть и иное альтернативное условие бесплатного получения доступа к услугам, без поведенческой рекламы (например, путем замены ее на иную рекламу)³⁰.

В приведенных разъяснениях в очередной раз делается акцент на необходимости обеспечения прозрачности и простоты предоставления информации; при этом соблюдение указанных требований фактически приводит к увеличению объема информации, обрушивающейся на субъекта данных, что снижает ее ценность, а ознакомление с ней становится еще одним неприятным препятствием к достижению цели. Поэтому представляется, что американский подход, предусматривающий право на отказ от обработки данных, является вполне жизнеспособным, поскольку предполагает осознанное поведение субъекта данных, которое он выражает в совершении активных действий. Безусловно, в таком случае имеет значение то, что соответствующая информация об использовании полностью автоматизированных систем и праве отказа от их применения должна привлекать внимание в рамках интерфейса сайта или приложения.

Условия применения полностью автоматизированных систем обработки данных без получе-

ния согласия субъекта данных могут быть определены в законодательстве отдельных стран ЕС при условии установления последними эффективных мер защиты прав, свобод и законных интересов субъекта данных. В комментарии 71 к Общему регламенту по защите данных ЕС определен минимальный перечень гарантий: право на получение конкретной информации, на вмешательство человека, на выражение точки зрения, на получение объяснения решения, принятого после такой оценки, и на оспаривание данного решения. Кроме того, на контролеров возлагается обязанность принимать технические и организационные меры для сведения к минимуму риска ошибок, обеспечения безопасности персональных данных. Соответствующие исключения из общего положения предусмотрены в законодательстве Австрии, Бельгии, Венгрии, Ирландии, Нидерландов, Словении, Франции и ФРГ.

Федеральный закон Австрии «О защите персональных данных»³¹ в § 41 определяет круг условий применения автоматизированных систем принятия решений: важнейшим критерием является соблюдение законности. Верховный административный суд Австрии в решении по делу о применении автоматизированной системы AMAS Государственной службой занятости Австрии отметил, что несмотря на тот факт, что такая система не принимает решение о мерах поддержки, результаты оценки ею соискателей ложатся в основу принятия решений работниками службы занятости, поэтому могут рассматриваться как полностью автоматизированные системы принятия решений. При этом суд подчеркнул, что «в настоящее время законодательство явно не содержит никаких положений, которые бы обосновывали возможность применять AMAS для обработки данных»³². В национальном законодательстве Австрии немного случаев, когда полностью автоматизированные системы могут применяться в отношении личности. Ф. Мерли к таким случаям относит принятие решений налоговыми органами³³. В федеральном законе «О грантах

³⁰ Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms. Adopted on 17 April 2024 // URL: https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf (дата обращения: 21.04.2024).

³¹ Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz — DSG), 1999 // BGBl. Nr. 165/1999. 17 August 1999.

³² Ro 2021/04/0010-11, 21 Dezember 2023.

³³ Merli F. Automated Decision-Making Systems in Austrian Administrative Law // Fascicolo. 2023. No. 1. P. 43. DOI: 10.13130/2723-9195/2023-1-19.

студентам»³⁴ также предусмотрено, что «решения, принятые с использованием автоматизированной обработки данных, не требуют подписи лица, выдавшего решение или удостоверение, и считаются утвержденными руководителем органа, выдающего студенческие гранты».

Федеральный закон Бельгии «О защите данных»³⁵ провозглашает, что «любое решение, основанное только на автоматизированной обработке... разрешено, если национальный закон, указ, постановление, закон ЕС или международное соглашение предусматривают соответствующие гарантии прав и свобод субъекта данных, по крайней мере право на вмешательство со стороны контролера». Как и в Австрии, законодательство Бельгии распространяет свое действие на случаи, которые не только ведут к правовым последствиям для субъекта данных, но и в целом могут существенно повлиять на него. Обращаясь к праву на вмешательство человека, Э. Ройг предостерегает от формализованного подхода: «Когда решение принимается на основе анализа данных, вмешательство человека не может изменить результат, если только оно не учитывает статистическую корреляцию... От сотрудника требуются знания в сфере аналитики данных, которые позволили бы ему отличать значимые корреляции от других, незначимых статистических связей, не имеющих никакой ценности для принятия решений»³⁶. В качестве попытки избежать формального подхода необходимо рассматривать положения Регламента ЕС «Об искусственном интеллекте», которые предусматривают обязанность оператора обеспечить работу системы под контролем субъекта, обладающего необходимыми знаниями. Полностью автоматизированные системы принятия решений внедрены в процесс аутентификации личности финансовыми учреждениями для получения доступа к учетной записи³⁷.

В Нидерландах сферы, в которых возможно использование автоматизированных систем принятия решений, определены Законом «О реализации Общего регламента по защите

данных»³⁸ целевыми условиями: «необходимо для соблюдения юридического обязательства, которому подчиняется контролер, или необходимо в общественных интересах». Таким образом, скоринг может применяться как органами публичной власти, так и частноправовыми субъектами. Административные органы самостоятельно выбирают меры защиты субъекта данных, в то время как частноправовые обязательно должны обеспечить реализацию по крайней мере трех правомочий: права на вмешательство человека, права выражать свою точку зрения и права оспаривать решение.

Особенности реализации права на доступ субъекта данных к информации, используемой в скоринговой модели

В рамках использования полностью автоматизированных систем принятия решений наиболее проблематичным является вопрос «черного ящика» и реализации права доступа субъекта данных к информации о скоринге. В Законе США «О добросовестной кредитной отчетности» «право знать» предусматривает право потребителя на получение информации о своем кредитном скоринге и андеррайтинге. По запросу потребителя агентство по отчетности должно раскрыть информацию о текущем кредитном скоринге лица, о его диапазонах в рамках используемого метода расчета, а также «все ключевые факторы, которые отрицательно повлияли на кредитный скоринг потребителя в используемой модели», дату формирования кредитного скоринга, наименование организации, предоставившей кредитный рейтинг или кредитное досье, а также указание на то, что рейтинг, используемый при принятии значимых решений, может отличаться от предоставленного. Запрос на предоставление кредитного скоринга не предполагает раскрытие математической модели, положенной в основу скоринга; таким образом, обеспечивается право

³⁴ Bundesrecht konsolidiert: Studienförderungsgesetz 1992 // BGBl. Nr. 305/1992. 26 Juni 1992.

³⁵ La Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, 2018.

³⁶ Roig A. Safeguards for the right not to be subject to a decision based solely on automated processing (Article 22 GDPR) // European Journal of Law and Technology. 2017. No. 8 (3). P. 6.

³⁷ La Loi du 11 mars 2018 relative au statut et au contrôle des établissements de paiement et des établissements de monnaie électronique, à l'accès à l'activité de prestataire de services de paiement et à l'activité d'émission de monnaie électronique, et à l'accès aux systèmes de paiement.

³⁸ Uitvoeringswet Algemene verordening gegevensbescherming, 25 mei 2018.

агентства сохранить коммерческую тайну, однако прозрачность входных данных, оказывающих влияние на принятое решение, является безусловной. В законодательстве штата Калифорния воспроизводится положение Общего регламента по защите данных ЕС: на оператора данных возлагается обязанность не только раскрывать факт использования автоматизированных систем обработки личной информации и принятия решения, но и «включать значимую информацию о логике принятия решений, а также описание вероятного результата процесса в отношении потребителя».

Внедрение технологий больших данных позволило массово обрабатывать «цифровые следы человека», которые могут как содержать персональные данные, так и отражать иные особенности человека, «которые несут информацию о его частной жизни»³⁹. Обработка цифровых следов, которые не содержат персональных данных, не предполагает необходимость соблюдения положений Общего регламента по защите данных ЕС или законодательства штатов США, однако в процессе обработки большого объема цифровых следов могут формироваться новые, так называемые производные персональные данные. Таким образом, разумно предполагать, что реализация права доступа означает, что субъект данных получает информацию об уже сформированных производных персональных данных, которые положены в основу скоринговой модели. Однако, анализируя положения Общего регламента по защите данных ЕС, А. Н. Мочалов отмечает, что ввиду отсутствия определенной концепции отнесения производных данных к субъекту данных или к контроллеру, который их создал, последний «может отказать субъекту в доступе к ним, ссылаясь, например, на то, что эта информация является коммерческой тайной»⁴⁰.

В феврале 2025 г. Европейский суд в решении по делу «Дан и Брэдстрит»⁴¹ разрешил правовую неопределенность в вопросе соотношения прав контроллера на защиту информации, относящейся к коммерческой тайне, и субъекта данных на получение доступа к информации

об использовании полностью автоматизированных систем обработки данных. Он указал, что субъект данных должен иметь доступ в том числе к входным данным, параметрам и входным переменным, используемым при оценке, и информации об их влиянии на рассчитанную оценку, о получении параметров или входных переменных, почему лицу присвоен определенный рейтинг, и пояснению того, какое требование было связано с этим рейтингом. Таким образом, производные персональные данные подлежат раскрытию; их можно рассматривать и как входные параметры, которые собраны в процессе профилирования, отделенном во времени от процесса скоринга, и как полученные параметры, если процессы профилирования и скоринга объединены во времени. Суд подчеркнул, что необходимость раскрытия всех обрабатываемых персональных данных обусловлена гарантированием права на проверку точности данных. Кроме того, он однозначно истолковал положение о раскрытии логики, которое еще совсем недавно вызывало дискуссии⁴², указав, что предполагается раскрытие в краткой, прозрачной, понятной и легкодоступной форме процедуры и принципов, специально применяемых к автоматизированной обработке персональных данных с целью получения определенного результата, например профиля платежеспособности. Предоставление самого алгоритма не соответствует требованиям краткости и понятности, поэтому математические формулы не подлежат раскрытию.

Иные гарантии прав человека при осуществлении скоринга

В условиях стремительного развития систем искусственного интеллекта особое значение приобретают вопросы обеспечения их безопасности в целом, поэтому регулирование отдельных аспектов их применения в отношении личности в рамках законодательства об обработке персональных данных становится недостаточным. Регламент Европейского Союза «Об искус-

³⁹ Мочалов А. Н. Цифровые следы человека и неприкосновенность частной жизни // Антиномии. 2024. № 24 (4). С. 172. DOI: 10.17506/26867206_2024_24_3_164.

⁴⁰ Mochalov A. N. Digital Profiling and the Legal Regime of Derived Personal Data // Kutafin Law Review. 2024. No. 11 (3). P. 502. DOI: 10.17803/27130533.2024.3.29.491-513.

⁴¹ Dun and Bradstreet, Austria. Case C-203/22, 2025.

⁴² Кузнецова С. С. Правовое регулирование цифрового профилирования человека в практике зарубежных стран // Правоприменение. 2024. № 8 (4). С. 66. DOI: 10.52468/2542-1514.2024.8(4).

ственном интеллекте» является важным шагом на пути обеспечения безопасности общества от угроз новых технологий. В рамках проблематики рейтингования личности с применением искусственного интеллекта данный акт имеет особую важность, так как, во-первых, устанавливает запрет на отдельные категории скоринга — социальный скоринг, а во-вторых, возлагает как на контролера данных, так и на третьих лиц (поставщика системы искусственного интеллекта) ряд дополнительных обязанностей.

Система искусственного интеллекта, которая выполняет профилирование физических лиц, всегда является высокорисковой, поэтому случаи, когда скоринг будет решением, принятым по результатам профилирования, подпадают под действие регламента о высокорисковых системах. В свою очередь скоринговые модели автоматизированного принятий решений сами по себе также отнесены к высокорисковым, даже когда они работают с входными данными о личности, заложенными человеком, если они используются в тех сферах, где их применение создает наибольшую угрозу правам человека (системы категоризации на основании биометрических данных, прием в образовательные учреждения, оценка результатов обучения, фильтрация и отбор заявлений о приеме на работу, оценка кандидата на соответствие занимаемой должности, принятие решений о продлении или прекращении трудовых отношений, принятие решений о предоставлении различных мер государственной поддержки, сферы кредитования и страхования, правосудие и т.д.).

В определении системы искусственного интеллекта выделены следующие ее ключевые критерии: демонстрирует адаптивность, т.е. подстраивается под задачи оператора; формирует выходные данные в виде прогнозов, решений, контента, рекомендаций на основе входных данных; выходные данные создаются как для явных, так и неявных целей и могут влиять на физическую или виртуальную среду. Подчеркивается, что системы искусственного интеллекта имеют разные уровни автономности, однако отмечается, что соответствующее понятие не охватывает системы, основанные на правилах, определенных исключительно физическими лицами для автоматического выполнения операций (п. 12 преамбулы Регламента ЕС «Об искусственном интеллекте»).

Наделение системы статусом высокорисковой возлагает как на ее поставщика, так и на оператора ряд обязанностей. Среди наиболее

значимых обязанностей поставщика, направленных на предотвращение и устранение рисков нарушения прав человека, можно выделить:

а) разработку системы управления рисками, нацеленную на выявление, анализ разумно предсказуемых рисков с учетом назначения системы, результатов мониторинга, опыта и знаний оператора и их устранение;

б) разработку и тестирование системы с использованием данных, которые отвечают требованиям их недискриминационности, безопасности, соответствия целям использования системы, пригодности и количества данных;

в) автоматическое ведение журналов событий;

г) обеспечение возможности контроля со стороны человека, в том числе путем предоставления оператору прозрачной и доступной информации о технических особенностях системы, назначении и возможных рисках и ограничениях, результатах предварительного тестирования, порядке интерпретации входных данных, а также возможности вмешательства в работу системы, в том числе путем ее остановки;

д) обеспечение надежности и устойчивости работы системы на протяжении всего периода жизненного цикла.

Операторы системы с высоким риском, в свою очередь, должны гарантировать компетентный человеческий надзор, принимать необходимые технические и организационные меры для обеспечения ее использования в соответствии с инструкциями, контролировать работу системы и информировать поставщика в случае выявления серьезных инцидентов или возможных рисков ее дальнейшего использования, обеспечивать релевантность, достаточность входных данных с учетом целей работы системы, информировать о ее внедрении лиц, которые подвергаются ее действию, а также проводить оценку воздействия на защиту данных.

Несмотря на то что Регламент ЕС «Об искусственном интеллекте» носит комплексный характер и направлен на минимизацию рисков применения систем искусственного интеллекта для принятия решений в отношении личности, представляется, что ряд вопросов по-прежнему остается нерешенным, например проблематика предвзятости системы. В названном Регламенте большое внимание уделяется вопросу разработки системы, в связи с чем на поставщика возлагается обязанность

по обеспечению ее обучения, тестирования с использованием полных, «качественных» данных. Однако, как справедливо отмечает Э. Бирн, возникновение предвзятости может быть связано не только с использованием при разработке системы данных, содержащих дискриминационные факторы, или разработкой алгоритма, который сам по себе содержит предвзятые условия, но и с процессом развертывания системы оператором⁴³.

И тут указанный Регламент по-прежнему возлагает всю ответственность на поставщика: с учетом того, что высокорисковые системы продолжают обучаться после ввода в эксплуатацию, он должен разрабатывать их таким образом, чтобы исключить или максимально снизить риск предвзятости, а также гарантировать, что любые такие циклы будут надлежащим образом устранены. Оператор, в свою очередь, несет крайне ограниченную ответственность в связи с возникновением предвзятости в работе системы, так как он должен лишь обеспечить надзор за ее работой лицом, которое в курсе возможной автоматической предвзятости высокорисковой системы. Представляется, что такое перекладывание полной ответственности на поставщика за обеспечение работы системы во время всего ее жизненного цикла является неэффективным, поскольку предвзятость может возникнуть в процессе нецелевой работы с ней оператора или в связи с отличием качества входных данных от тех, что использовал поставщик. Американский подход, предложенный Нью-Йорком⁴⁴, наиболее логичен, так как возлагает на пользователя системы-работодателя обязанность по проведению ежегодного независимого аудита на наличие предвзятости, дискриминации в ее работе. В таком случае риски нарушения прав человека в связи с недостаточной компетентностью оператора системы могут быть минимизированы.

Законодательство штатов США, регламентирующее условия использования систем и моделей искусственного интеллекта с целью скоринга, крайне разнообразно. Так, например, в штате Нью-Йорк запрещено их применение в деятельности органов власти в целях принятия решений о предоставлении мер социаль-

ной поддержки⁴⁵. В штате Колорадо с 1 января 2026 г. вступят в действие поправки к Закону «О защите конфиденциальности потребителей», которые дополняют его разделом «Искусственный интеллект». Данные поправки налагают на оператора системы искусственного интеллекта обязанность проводить оценку рисков и дискриминационной вероятности, а также, как в законе штата Калифорния, предоставлять информацию о целях работы системы искусственного интеллекта, о характере решений, о порядке реализации права отказаться от обработки персональных данных, о том, какие сведения ложатся в основу автоматизированного принятия решений в случае неблагоприятных решений, об источниках получения этих данных, порядке их оценки системой и обжалования решений. Стремясь обеспечить справедливость принимаемых моделями искусственного интеллекта решений, штат Калифорния предусмотрел необходимость раскрытия поставщиком информации об использованных для обучения данных: об источниках и владельцах наборов данных; о том, как наборы данных способствуют достижению предполагаемой цели системы; о том, использовались ли личная информация или объекты авторского права, и т.д. При таком регулировании в очередной раз встает вопрос о балансе интересов субъекта данных и поставщика, желающего сохранить коммерческую тайну.

Заключение

Четвертая промышленная революция практически бесконечно расширяет возможности человека и общества в ускорении, повышении эффективности обработки информации. Однако развитие информационных технологий становится вызовом для человека, его прав и свобод, поэтому эффективное правовое регулирование оснований и порядка использования автоматизированных систем принятия решений в отношении личности является одной из первоочередных задач. Анализ регулятивной практики скоринга личности в США и Европейском Союзе позволяет сформулировать следующие критерии эффективного правового регулирования:

⁴³ Byrne A., Lee D., Le Q. Bias in AI: tackling the issues through regulations and standards. October 14, 2024 // URL: <https://publicpolicy.ie/papers/bias-in-ai-tackling-the-issues-through-regulations-and-standards/> (дата обращения: 28.04.2024).

⁴⁴ New York City Local Law 144 of 2021.

⁴⁵ New York Loading Act 403 of 2024.

1) универсализация подхода к однородным процессам. Правовое регулирование обработки данных личности с применением автоматизированных скоринговых моделей в США неоднородно, осуществляется на двух уровнях государственной власти; при этом сфера действия соответствующих актов зависит от субъектного состава правоотношения. Такая модель правового регулирования приводит к образованию пробелов, что хорошо демонстрируется наличием вредоносной практики брокеров данных; вместе с тем резиденты большинства штатов США зачастую остаются наедине с проблемой использования в отношении них технологий автоматизированной обработки данных. Европейский подход можно рассматривать как более гармоничный, обеспечивающий формирование однородной и понятной для субъектов правоотношений правоприменительной практики;

2) переосмысление согласия как наиболее эффективного средства защиты прав личности. Пользователи онлайн-пространства в условиях переизбытка информации зачастую рассматривают «выскакивающие» предложения о предоставлении согласия на обработку данных с использованием автоматизированных систем как дополнительный ненужный шум и дают такое согласие без необходимого осмысления. Другие, как отмечают исследователи, считают, что полностью автоматизированные системы являются менее дискриминационными, и предпочитают их людям для принятия решений. Поэтому, на наш взгляд, концепция получения согласия, особенно в онлайн-пространстве, на сегодняшний день утратила свою ценность, и американский подход предоставления права на отказ от использования автоматизированных систем является оправданным;

3) поиск баланса интересов субъекта данных и оператора. В условиях использования полностью автоматизированных систем принятия решений абсолютная прозрачность представляется фикцией. С одной стороны, борьба с дискриминацией и предвзятостью автоматизированных систем требует максимальной от-

крытости порядка принятия решений, однако, с другой стороны, необходимо помнить и о законных ожиданиях оператора данных в отношении защиты коммерческой тайны. На сегодняшний день в странах ЕС и США укоренилась практика, которая предусматривает необходимость раскрытия субъекту информации о том, какие данные и критерии были положены в основу принятия решений, в том числе объяснения причин негативного для человека решения. Эта практика представляется вполне логичной, однако возникает сомнение в том, что такой подход обеспечивает реальную прозрачность, поскольку при использовании системы искусственного интеллекта, способной к машинному обучению, алгоритмы принятия решений тоже могут меняться. Данные меры должны подкрепляться постоянным мониторингом самой системы искусственного интеллекта с позиции ее предвзятости;

4) комплексность регулирования процессов разработки и внедрения систем искусственного интеллекта в процессы, связанные с принятием решений в отношении личности. Добросовестное поведение оператора данных, выражающееся в строгом исполнении норм законодательства о защите персональных данных в процессе использования алгоритмов профилирования и скоринга, является недостаточным ввиду серьезной автономности алгоритмических систем. Поэтому акты, направленные на регулирование отдельных вопросов разработки и внедрения систем искусственного интеллекта в ЕС и США, являются своевременными. Однако, несмотря на достаточно передовой опыт правового регулирования ЕС, который, безусловно, требует осмысления и использования для совершенствования соответствующего законодательства РФ, в Регламенте «Об искусственном интеллекте» тоже имеются пробелы, которые не позволяют обеспечить эффективную работу скоринговых моделей как высокорисковых систем. К таким проблемам, например, относится недостаточное урегулирование обязанностей оператора системы.

СПИСОК ЛИТЕРАТУРЫ

Агафонова В. В., Вишневер В. Я., Фрумусак С. В. Технологическая эволюция кредитного скоринга в системе банковского потребительского кредитования // Вестник Волжского университета имени В.Н. Татищева. 2018. Т. 2. № 3. С. 21–26.

Вилкова О. В. К вопросу о научной осмысленности применения веб-скрейпинга как метода сбора данных в социологических исследованиях // Вестник Томского государственного университета. Философия. Социология. Политология. 2020. № 54. С. 163–175. DOI: 10.17223/1998863X/54/16.

Кузнецова С. С. Правовое регулирование цифрового профилирования человека в практике зарубежных стран // Правоприменение. 2024. № 8 (4). С. 63–72. DOI: 10.52468/2542-1514.2024.8(4).

Луняков О. В., Лунякова Н. А. Развитие каналов кредитования в условиях перехода к цифровой экономике: моделирование спроса // Финансы: теория и практика. 2018. № 22 (5). С. 76–89. DOI: 10.26794/2587-5671-2018-22-5-76-89.

Мочалов А. Н. Парадокс анонимности в Интернете и проблемы его правового регулирования // Вестник СурГУ. 2021. № 4 (34). С. 111–121.

Мочалов А. Н. Цифровые следы человека и неприкосновенность частной жизни // Антиномии. 2024. № 24 (4). С. 164–189. DOI: 10.17506/26867206_2024_24_3_164.

Рувинский Р. З. Правовые аспекты внедрения системы социального кредита в современное публичное управление. Н. Новгород : НИУ РАНХиГС, 2022. 264 с.

Abrusio J. The (In)Efficacy of Consent for the Processing of Personal Data // Global Network Journal. 2024. No. 6 (1). P. 180–205. DOI: 10.24861/2675-1038.v6i1.133.

Berg T., Burg V., Gombović A., Puri M. On the Rise of FinTechs — Credit Scoring Using Digital Footprints // The Review of Financial Studies. 2020. No. 7. P. 2845–2897.

Bertrand M., Kamenica E. Coming apart? Lives of the rich and poor over time in the United States. Chicago, 2017.

Desai N., Gross J. Scoring systems in the critically ill: uses, cautions, and future directions // BJA Education. 2019. No. 19 (7). P. 212–218. DOI: 10.1016/j.bjae.2019.03.002.

Germundsson N., Stranz H. Automating social assistance: Exploring the use of robotic process automation in the Swedish personal social services // International Journal of Social Welfare. 2023. No. 33 (17). P. 1–12. DOI: 10.1111/ijsw.12633.

Martin K. Privacy Notices as Tabula Rasa: An Empirical Investigation into How Complying with a Privacy Notice is Related to Meeting Privacy Expectations Online // Journal of Public Policy & Marketing. 2015. Vol. 34 (2). P. 68–85. DOI: 10.1509/jppm.14.139.

Merli F. Automated Decision-Making Systems in Austrian Administrative Law // Fascicolo. 2023. No. 1. P. 41–50. DOI: 10.13130/2723-9195/2023-1-19.

Mochalov A. N. Digital Profiling and the Legal Regime of Derived Personal Data // Kutafin Law Review. 2024. No. 11 (3). P. 491–513. DOI: 10.17803/27130533.2024.3.29.491-513.

Roig A. Safeguards for the right not to be subject to a decision based solely on automated processing (Article 22 GDPR) // European Journal of Law and Technology. 2017. No. 8 (3). P. 1–17.

Obar J. A., Oeldorf-Hirsch A. The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services // Information, Communication & Society. 2018. No. 23 (1). P. 128–147. DOI: 10.1080/1369118X.2018.1486870.

Rice L., Swesnik D. Discriminatory Effects of Credit Scoring on Communities of Color. National Fair Housing Alliance, 2012. 29 p.

Sherman J. Data Brokers and Sensitive Data on U. S. Individuals: Threats to American Civil Rights, National Security, and Democracy. Durham, 2021. 16 p.

REFERENCES

Abrusio J. The (In)Efficacy of Consent for the Processing of Personal Data. *Global Network Journal*. 2024;6(1):180-205. DOI: 10.24861/2675-1038.v6i1.133.

Agafonova VV, Vishnever VYa, Frumusaki SV. Technological evolution of credit scoring in the consumer banking lending system. *Vestnik Volzhskogo Universiteta imeni V.N. Tatishcheva*. 2018;2(3):21-26. (In Russ.).

Berg T, Burg V, Gombović A, Puri M. On the Rise of FinTechs — Credit Scoring Using Digital Footprints. *The Review of Financial Studies*. 2020;7:2845-2897.

Bertrand M, Kamenica E. Coming apart? Lives of the rich and poor over time in the United States. Chicago; 2017.

Desai N, Gross J. Scoring systems in the critically ill: uses, cautions, and future directions. *BJA Education*. 2019;19(7):212-218. DOI: 10.1016/j.bjae.2019.03.002.

Germundsson N, Stranz H. Automating social assistance: Exploring the use of robotic process automation in the Swedish personal social services. *International Journal of Social Welfare*. 2023. P. 1–12. DOI: 10.1111/ijsw.12633.

Kuznetsova SS. Legal regulation of digital human profiling in the practice of foreign countries. *Pravoprimenenie*. 2024;8(4):63-72. DOI: 10.52468/2542-1514.2024.8(4). (In Russ.).

Lunyakov OV, Lunyakova NA. Development of credit channels in the context of the transition to the digital economy: Demand modeling. *Finansy: teoriya i praktika [Finance: Theory and practice]*. 2018;22(5):76-89. DOI: 10.26794/2587-5671-2018-22-5-76-89. (In Russ.).

Martin K. Privacy notices as Tabula Rasa: An Empirical Investigation into How Complying with a Privacy Notice is Related to Meeting Privacy Expectations Online. *Journal of Public Policy & Marketing*. 2014. P. 68–85. DOI: 10.1509/jppm.14.139.

Merli F. Automated Decision-Making Systems in Austrian Administrative Law. *Fascicolo*. 2023;1:41-50. DOI: 10.13130/2723-9195/2023-1-19.

Mochalov AN. Digital Profiling and the Legal Regime of Derived Personal Data. *Kutafin Law Review*. 2024;11(3):491-513. DOI: 10.17803/27130533.2024.3.29.491-513.

Mochalov AN. Human digital footprints and privacy. *Antinomii [Antinomies]*. 2024;24(4):164-189. DOI: 10.17506/26867206_2024_24_3_164. (In Russ.).

Mochalov AN. The paradox of anonymity on the Internet and the problems of its legal regulation. *Vestnik SurGU*. 2021;4(34):111-121. (In Russ.).

Obar JA, Oeldorf-Hirsch A. The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*. 2018;23(1):128-147. DOI: 10.1080/1369118X.2018.1486870.

Rice L, Swesnik D. Discriminatory Effects of Credit Scoring on Communities of Color. National Fair Housing Alliance; 2012.

Roig A. Safeguards for the right not to be subject to a decision based solely on automated processing (Article 22 GDPR). *European Journal of Law and Technology*. 2017;8(3):1-17.

Ruvinsky RZ. Legal aspects of the introduction of the social credit system in modern public administration. N. Novgorod: NIU RANHiGS Publ.; 2022. (In Russ.).

Sherman J. Data Brokers and Sensitive Data on U. S. Individuals Threats to American Civil Rights, National Security, and Democracy. Durham; 2021.

Vilkova OV. On the issue of the scientific meaningfulness of the use of web scraping as a data collection method in sociological research. *Vestnik Tomskogo gosudarstvennogo universiteta. Filosofiya. Sotsiologiya. Politologiya [Tomsk State University Journal. Philosophy. Sociology. Political science]*. 2020;54:63-175. DOI: 10.17223/1998863X/54/16. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Кузнецова Светлана Сергеевна, кандидат юридических наук, доцент, доцент кафедры конституционного права Уральского государственного юридического университета имени В.Ф. Яковлева
д. 21, Комсомольская ул., г. Екатеринбург 620066, Российская Федерация
kss001@usla.ru

INFORMATION ABOUT THE AUTHOR

Svetlana S. Kuznetsova, Cand. Sci. (Law), Associate Professor, Associate Professor, Department of Constitutional Law, Ural State Law University named after V.F. Yakovlev, Ekaterinburg, Russian Federation
kss001@usla.ru

Материал поступил в редакцию 7 мая 2024 г.

Статья получена после рецензирования 9 мая 2025 г.

Принята к печати 15 сентября 2025 г.

Received 07.05.2024.

Revised 09.05.2025.

Accepted 15.09.2025.