

ПОДХОДЫ К ПРАВОВОМУ РЕГУЛИРОВАНИЮ ОТНОШЕНИЙ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРАВООХРАНЕ

О.А. Степанов, М.М. Степанов

Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации, г. Москва, Россия

Информация о статье

Дата поступления –
11 декабря 2024 г.
Дата принятия в печать –
20 сентября 2025 г.
Дата онлайн-размещения –
20 декабря 2025 г.

Исследуются подходы к правовому регулированию отношений, связанных с использованием искусственного интеллекта в правоохране. Делается выводы об особенностях такого регулирования с точки зрения результатов правоприменения в Китае (восточный подход), а также в США и европейских странах (западный подход). Особое внимание уделяется необходимости обеспечения защиты прав граждан в процессе сбора информации о них, ее обработки и учета решений, подготовленных искусственным интеллектом для должностных лиц органов правоохраны, в Российской Федерации. Эти обстоятельства предполагают создание механизма обжалования данных решений путем разработки и принятия соответствующих норм права.

Ключевые слова

Искусственный интеллект,
правоохрана, Российская
Федерация, правовое
регулирование, восточный
подход, западный подход,
защита прав граждан, правовой
механизм обжалования
решений

APPROACHES TO THE LEGAL REGULATION OF ARTIFICIAL INTELLIGENCE APPLICATION IN LAW ENFORCEMENT

Oleg A. Stepanov, Mikhail M. Stepanov

Institute of Legislation and Comparative Law under the Government of the Russian Federation,
Moscow, Russia

Article info

Received –
2024 December 11
Accepted –
2025 September 20
Available online –
2025 December 20

The article considers the Eastern (People's Republic of China) and Western (USA, European countries) approaches to the legal regulation of relations related to the use of artificial intelligence in law enforcement.

The subject of the study is the relations arising in the process of such regulation. The purpose of the study is to analyze the legal regulation of the use of artificial intelligence in the process of collecting information about citizens, its processing and taking into account the decisions prepared by AI for law enforcement officials.

The methodological basis of the study is logical and systematic methods of scientific cognition, as well as methods of analysis and synthesis of legal phenomena.

Foreign and domestic experience of legal regulation is studied. Special attention is paid to the need to ensure the protection of citizens' rights in the process of collecting information about them, its processing and taking into account the decisions prepared by artificial intelligence for law enforcement officials. It is pointed out that the peculiarities of legal regulation in this sphere of life activity of society are conditioned by the correctness of conclusions formulated by artificial intelligence, as well as the competence of algorithm developers and persons carrying out its training. Legal regulation of the relevant relations is considered through the prism of the results of law enforcement. The Eastern approach assumes the assessment of the actions of individuals by a number of parameters, taking into account which their trustworthiness index is determined, implying the assignment of a personal id to them personal identification code (social rating). The Western approach is that the United States and Western states actively using digital control tools based on AI technologies in the field of law enforcement do not inform the population about the total

Keywords

Artificial intelligence, law
enforcement, Russian Federation,
legal regulation, Eastern approach,
Western approach, protection
of citizens' rights, legal mechanism
of appealing decisions

surveillance of people. It is noted that at present the regulation of this sphere in the Russian Federation is more oriented to the Western approach. At the same time, at the national level there is no mechanism of legal regulation on the consequences of actions of a person in the field of law enforcement. Attention is drawn to the fact that while in China for “unreliable” persons only a number of restrictions are imposed on their movement (use of airplanes and trains), occupation (prohibition to hold managerial positions in certain areas), obtaining financial services (refusal to issue loans), in the United States such persons are placed without trial in secret prisons, where they are tortured.

It is concluded that taking into account this circumstance requires the creation in the Russian Federation of a legal mechanism for appealing decisions taken by law enforcement officials on the basis of recommendations developed by artificial intelligence, by developing and adopting norms of law to prevent the use of its potential for purposes incompatible with the goals of law enforcement. This implies the need to develop a system of theoretical ideas about the most rational forms and methods of legal regulation in considering.

1. Введение

Рост массивов данных и развитие алгоритмических технологий влечет за собой разработку новых способов контроля над населением (политического, экономического, социального) [1, с. 420], связанных с анализом разнородных и неструктурированных данных о гражданах на основе технологии *Big Data* [2–5]. Важнейшей характеристикой этой технологии является использование искусственного интеллекта (далее – ИИ).

Поскольку *Big Data* и ИИ широко применяются в правоохранительной деятельности, в современных условиях становятся актуальными как сама возможность использования инновационных продуктов в деятельности правоохранительных органов, так и соответствующая правовая регламентация.

В настоящее время наметились два основных подхода к правовому регулированию отношений, связанных с использованием ИИ в сфере правоохранительной деятельности. Условно их можно обозначить как *восточный* (Китайская Народная Республика; далее также – КНР) и *западный* (США, европейские страны).

2. Опыт Китайской Народной Республики

В КНР интересы общества, основанные на традиционных ценностях, являются приоритетными по сравнению с интересами личности, ее индивидуальными правами и свободами. Эта тенденция прослеживается и в правовом регулировании отношений, связанных с использованием ИИ в сфере правоохраны.

При этом следует отметить, что развитию ИИ в КНР уделяется повышенное внимание. Еще в 2017 г.

Госсоветом КНР был принят План развития искусственного интеллекта нового поколения¹, в котором закреплялось, что к 2030 г. Китай должен достичь ведущего мирового уровня в общей теории, технологии и применении ИИ, стать крупнейшим в мире инновационным центром ИИ, а также достичь значительных результатов в «умной» экономике и «умном обществе».

Использование ИИ в общественном и государственном управлении, а также в целях правоохраны в Китае осуществляется в рамках развития системы социального кредита (система социального рейтинга, система социального доверия), которая в настоящее время с различной степенью готовности введена в действие на региональном уровне. На данный момент она считается наиболее крупной и сложной в мире структурой мониторинга и последующего воздействия на поведение как отдельных индивидов, так и социума в целом. Ее создание началось 14 июня 2014 г., когда Госсовет КНР принял План строительства системы социального кредита (2014–2020)². В развитие Плана на местном уровне принимаются свои нормативные правовые акты [6].

В отечественной литературе отмечается, что одной из целей разработки и внедрения системы социального кредита стало изменение общественной ситуации в стране и необходимость ее стабилизации. Поскольку традиционные практики охранительного реагирования на протестное движение в Китае, сложившиеся ранее, себя исчерпали, то введение системы социального кредита стало рассматриваться в качестве инструмента контроля над поведением людей, борьбы с преступностью, расследова-

¹ URL: https://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm (дата обращения: 11.12.2024).

² URL: http://www.gov.cn/zhengce/content/2014-06/27/content_8913.htm (дата обращения: 11.12.2024).

ния преступлений и правонарушений [7, с. 82], оказывающего влияние на законопослушность граждан [8, с. 105].

Данная система связана с оцениванием действий физических лиц по ряду параметров, на основании которых определяется их индекс благонадежности (социальный рейтинг). Поэтому ее основой является сбор и обработка информации о субъекте. Эта деятельность осуществляется как на уровне Правительства КНР, так и на уровне отдельных регионов. Для удобства обработки данных каждому физическому лицу в соответствии с принятым еще в 2003 г. Законом об удостоверении личности гражданина КНР был присвоен персональный идентификационный код (номер удостоверения)³.

Сегодня 18-значный идентификационный код личности необходим для получения государственных услуг, применения электронных платежных систем, осуществления покупок в онлайн-магазинах, оформления проездных документов, приобретения сим-карт, регистрации в качестве интернет-пользователей и пр. [9; 10]. Информация об его использовании собирается, обрабатывается и хранится. На ее основе формируются досье физических лиц, которые хранятся в соответствующей кредитной платформе [11, с. 151].

Наряду с этим получение данных о гражданах Китая осуществляется с помощью SMART-гаджетов [12]. Например, в смартфоны при продаже устанавливаются обязательные приложения, отслеживающие передвижение человека, его покупки, заказы, платежи, состояние здоровья, контакты, активность в соцсетях и Интернете и мн. др. При этом следует учитывать, что в Китае каждый телефон, как и SIM-карта, привязан к его владельцу, личность которого идентифицирована [13].

Значимым источником информации о поведении жителей КНР в публичном пространстве являются камеры видеонаблюдения. С целью идентификации любого китайского гражданина по его фотографии на удостоверении личности в Китае был реализован проект видеонаблюдения *Sharp Eyes* («Острые глаза»). В рамках этого проекта к 2020 г. в КНР предполагалось

установить 626 млн камер видеонаблюдения⁴, информацию с которых обрабатывал ИИ. В настоящее время система видеонаблюдения в Китае продолжает развиваться [14, с. 40], в том числе в направлении распознавания камерами лиц, скрытых защитными медицинскими масками, ношение которых существенно снизило ее эффективность [15, с. 133].

Доступ к уличным камерам в КНР имеют не только правоохранительные и иные государственные органы, но и обычные граждане, которые с помощью специальных телевизионных приставок и смартфонов могут к ним подключиться в реальном времени и в случае обнаружения какого-либо правонарушения сообщить об этом полиции.

Камеры видеонаблюдения используются в Китае совместно с технологией распознавания лиц, что позволяет в автоматическом режиме осуществлять поиск находящихся в розыске правонарушителей. Кроме того, сотрудники правоохранительных органов и спецслужб в местах, где камеры отсутствуют или их деятельность затруднена, применяют очки, оснащенные данной технологией. Использование этих технологических решений значительно повышает эффективность обнаружения разыскиваемых⁵.

Интересно отметить, что в результате работы камер видеонаблюдения, оснащенных технологией ИИ, в период с 2012 по 2016 г. преступность по восьми видам тяжких преступлений, включая незаконный оборот наркотиков, кражу и умышленное причинение телесных повреждений, в Китае снизилась на 42,7 %⁶.

Среди региональных систем социального кредита выделяется система, внедренная в Синьцзян-Уйгурском автономном районе (далее – СУАР). Ее главными особенностями являются усиленный контроль над поведением граждан и направленность на выполнение правоохранительной функции. В связи с этим у жителей СУАР были получены образцы ДНК и голоса, а также сканирована радужная оболочка глаз. Все видеокамеры в СУАР интегрированы в единую систему. Кроме того, информация снимается с GPS-трекеров в автомобилях, сканеров распознавания лиц на контрольно-пропускных пунктах и круп-

³ URL: https://baike.baidu.com/item/中华人民共和国居民身份证法/182464?fromModule=lemma_inlink#3 (дата обращения: 11.12.2024).

⁴ Hersey F. China to have 626 million surveillance cameras within 3 years // TechNode. Nov. 22, 2017. URL: <https://technode.com/2017/11/22/china-to-have-626-million-surveillance-cameras-within-3-years/>.

⁵ Mozur P. Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras // The New York Times. July 8, 2018. URL: <https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html>.

⁶ Facial recognition, AI and big data poised to boost Chinese public safety // Global Times. Oct. 17, 2017. URL: <http://en.people.cn/n3/2017/1017/c90000-9280772.html>.

ных общественных объектах. Специальные приложения на смартфонах фиксируют вызывающие подозрения сообщения и записи. В результате внедрения системы в СУАР произошло определенное снижение уровня экстремизма [16].

Следует отметить, что на территории Китая не удалось реализовать в полном объеме идею социального рейтинга – это сделано с учетом экономических возможностей лишь на территории отдельных провинций. Поэтому в настоящее время система социального кредита в КНР с территориальной и правоприменительной точек зрения носит фрагментарный характер [17, с. 18]. Она представляет собой десятки pilotных проектов, внедряемых на местах властями различных уровней и коммерческими организациями [18, с. 68–69], отличающихся друг от друга по содержанию, правовому регулированию и степени контроля над поведением населения на основе сбора информации о гражданах и формирования их цифровых личностей [19–21].

3. Опыт США и европейских стран

Для западного подхода к регулированию использования ИИ в правоохранительной деятельности характерно то, что в США и европейских странах инструменты цифрового контроля, основанные на технологиях ИИ, также активно используются в сфере правоохраны, но население о ведении за ним тотального наблюдения в известность не ставится.

О наличии соответствующих программ стало широко известно в июне 2013 г. после опубликования секретных сведений, переданных в прессу аналитиком Агентства национальной безопасности США Э. Сноуденом.

В рамках реализации проектов *PRISM*, *XKeyscore*, *Tempora* и др. спецслужбы США и их союзников осуществляют контроль над информацией, передаваемой с помощью различных средств коммуникации как американскими гражданами, так и гражданами других государств, с целью выявления

неблагонадежных лиц, потенциальных террористов и лиц, уже совершивших преступления.

Проводимая странами Запада слежка за населением планеты приобрела такие масштабы, что стала предметом разбирательства в структурах Организации Объединенных Наций. По этому поводу были вынесены резолюции Генеральной Ассамблеи ООН A/RES/68/167 от 18 декабря 2013 г.⁷ и A/RES/69/166 от 18 декабря 2014 г.⁸ В них содержались призывы к государствам положить конец нарушениям прав человека, пересмотреть национальное законодательство, в том числе регулирующее отношения в области слежения за сообщениями, их перехвата и сбора личных данных, и привести его в соответствие с международным правом в области прав человека.

В докладах Управления Верховного комиссара ООН по правам человека от 30 июня 2014 г. A/HRC/27/37 и от 19 декабря 2014 г. A/HRC/28/39, посвященных проблемам нарушения прав человека при слежении с помощью цифровых коммуникационных технологий (интернет, мобильные телефоны, смартфоны, устройства с поддержкой Wi-Fi), перехвата и сбора содержащихся в них данных, рассматривались вопросы защиты права на неприкосновенность частной жизни в контексте национального и экстерриториального наблюдения, а также о перехвате и сборе личных данных, в том числе в массовом масштабе⁹.

Следует отметить, что США и Великобритания являются первоходцами в использовании систем видеонаблюдения в целях обеспечения общественного порядка [22, р. 136]. В настоящее время количество видеокамер в странах Запада увеличивается, совершенствуется их программное обеспечение, в том числе в направлении внедрения продуктов на основе ИИ. Развитие интеллектуальных систем видеонаблюдения позволило даже говорить о возникновении на Западе «государства наблюдения» («государства слежки»)¹⁰.

⁷ Резолюция Генеральной Ассамблеи ООН от 18 декабря 2013 г. A/RES/68/167 «Право на неприкосновенность личной жизни в цифровой век». URL: <https://undocs.org/ru/A/RES/68/167> (дата обращения: 11.12.2024).

⁸ Резолюция Генеральной Ассамблеи ООН от 18 декабря 2014 г. A/RES/69/166 «Право на неприкосновенность личной жизни в эпоху цифровых технологий». URL: <https://undocs.org/ru/A/RES/69/166> (дата обращения: 11.12.2024).

⁹ Доклад Управления Верховного комиссара ООН по правам человека от 30 июня 2014 г. A/HRC/27/37 «Право на неприкосновенность личной жизни в цифровой век». URL: <https://undocs.org/ru/A/HRC/27/37> (дата обращения:

11.12.2024); Доклад Управления Верховного комиссара ООН по правам человека от 19 декабря 2014 г. A/HRC/28/39 «Резюме обсуждения на дискуссионном форуме вопроса о праве на неприкосновенность частной жизни в цифровой век». URL: <https://www.undocs.org/ru/A/HRC/28/39> (дата обращения: 11.12.2024).

¹⁰ Devlin H. «We are hurtling Towards a Surveillance State»: The Rise of Facial Recognition Technology // The Guardian. Oct. 5, 2019. URL: <https://www.theguardian.com/technology/2019/oct/05/facial-recognition-technology-hurtling-towards-surveillance-state>.

Собранные на граждан данные анализируются различными программами, в основе которых лежат технологии ИИ. Лидером в этой области является компания *Palantir* (*Palantir Technologies, Inc.*). Первоначально ее главным заказчиком и инвестором стало ЦРУ. Впоследствии программные продукты *Palantir* стали использовать различные военные структуры, правоохранительные и специальные службы, в том числе ЦРУ, ФБР, полиция. Например, программное обеспечение *Palantir* в настоящее время широко применяется в работе полицейского управления Лос-Анджелеса¹¹.

Таким образом, в США и европейских странах также осуществляется сбор и обработка персональных данных населения в целях правоохраны. При этом широко используются возможности ИИ. Однако, в отличие от Китая, данная информация скрыта от граждан, которые практически не осведомлены об этой стороне деятельности государства. Отсутствуют официально опубликованные нормативные правовые акты, регламентирующие ее, а также механизм защиты прав граждан в процессе ее осуществления.

Вследствие этого, например, 25 мая 2021 г. Европейский Суд по правам человека вынес постановление по делу «Организация *Big Brother Watch* и другие против Соединенного Королевства». Суд пришел к выводу, что Великобританией была нарушена Европейская конвенция о защите прав человека и основных свобод, поскольку она активно занималась перехватом коммуникационных данных своих граждан (звонков, СМС-сообщений, электронной переписки и т. д.) и неправомерным получением информации о пользователях у провайдеров коммуникационных услуг¹². Однако дальнейшего развития, кроме констатации указанных фактов, эта ситуация не получила.

4. Опыт Российской Федерации

Реалии использования ИИ в отечественной сфере правоохраны позволяют сделать вывод о том, что в настоящее время правовое регулирование в большей степени ориентировано на западный подход к этим отношениям.

¹¹ Burns M. Leaked Palantir Doc Reveals Uses, Specific Functions And Key Clients // Techcrunch. Jan. 11, 2015. URL: <https://techcrunch.com/2015/01/11/leaked-palantir-doc-reveals-uses-specific-functions-and-key-clients/>.

¹² Постановление Европейского Суда по правам человека от 25 мая 2021 г. по делу «Организация *Big Brother Watch* и другие против Соединенного Королевства» (Жалоба № 58170/13 и две другие жалобы) // Бюллетень Европейского Суда по правам человека: рос. изд. М., 2022. № 1 (235).

Сбор данных о населении страны ведется постоянно. Правовой основой данной деятельности является прежде всего Федеральный закон от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон “О противодействии терроризму” и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»¹³. Статья 13 данного федерального закона внесла изменения в Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи»¹⁴, возложив на операторов связи обязанность по хранению на территории Российской Федерации информации о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи – в течение трех лет; а текстовых сообщений, голосовой информации, изображений, звуков, видео-, иных сообщений пользователей услугами связи – до шести месяцев. Согласно ст. 15 указанного федерального закона были внесены изменения в Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»¹⁵, обязывающие организаторов распространения информации в сети «Интернет» хранить на территории Российской Федерации информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей сети и информацию об этих пользователях – в течение одного года; текстовые сообщения пользователей сети, голосовую информацию, изображения, звуки, видео-, иные электронные сообщения – до шести месяцев.

Кроме того, для сбора информации применяются различные виды программ СОРМ (Система технических средств для обеспечения функций оперативно-розыскных мероприятий)¹⁶, программа «Камертон» и др. При этом интересно отметить, что еще в 2015 г. по факту применения СОРМ Европейским Судом по правам человека было принято решение о

¹³ Собрание законодательства Российской Федерации. 2016. № 28. Ст. 4558.

¹⁴ Собрание законодательства Российской Федерации. 2003. № 28. Ст. 2895.

¹⁵ Собрание законодательства Российской Федерации. 2006. № 31 (ч. I). Ст. 3448.

¹⁶ См.: Приказ Государственного комитета Российской Федерации по связи и информатизации от 20 апреля 1999 г. № 70 «О технических требованиях к системе технических

том, что работа данной системы (согласно ст. 8 Конвенции о защите прав человека и основных свобод) нарушает право на уважение частной и семейной жизни¹⁷.

Еще одним источником получения информации о населении России, используемым в правоохранительной деятельности, являются данные, получаемые в результате работы камер видеонаблюдения и их обработки ИИ. Правовое регулирование этой деятельности осуществляется субъектами Российской Федерации самостоятельно. Например, 7 февраля 2012 г. Правительством Москвы было принято Постановление № 24-ПП «Об утверждении Положения о государственной информационной системе “Единый центр хранения и обработки данных”»¹⁸. Камеры этой информационной системы в настоящее время установлены во дворах, подъездах, местах массового скопления людей и других местах. В 2021 г. Москва вошла в топ-30 мегаполисов мира по числу камер видеонаблюдения на квадратный километр. В настоящее время их установлено более 227 200. Информация с них была использована при расследовании 70 % преступлений¹⁹.

Следует отметить, что российские компании, работающие в области видеоаналитики, являются одними из ведущих в мире. Программные продукты, создаваемые ими, нередко превосходят зарубежные аналоги. Так, использование антитеррор-системы на основе технологий лицевой биометрии *FindFace*, которая является частью системы «Безопасный город», позволяет мгновенно идентифицировать правонарушителей на территории Москвы, выявлять оружие и другие объекты, устанавливать местонахождение разыскиваемых лиц. Программа имеет мобильное приложение, которое позволяет пользоваться всем спектром ее функций сотрудникам полиции из любой точки города. Для патрулирования улиц или массовых мероприятий есть возможность подключать камеры мобильных телефонов и

очки дополненной реальности. По фото- или видеоматериалам, изъятым с места преступления (например, с камеры банкомата или из системы охранного видеонаблюдения), программа *FindFace* позволяет установить место проживания разыскиваемого, маршруты его передвижения, выявить его социальные связи, в том числе потенциальных сообщников, и получить другую ценную оперативную информацию.

Во время проведения матчей Чемпионата мира по футболу 2018 г. в России использование системы *FindFace Multi* позволило успешно распознать и принять своевременные меры к задержанию порядка 100 человек из 50 000 разыскиваемых по фотографиям правонарушителей, в том числе находящихся в федеральном розыске, экстремистов и футбольных фанатов (включая зарубежных) с запретом на посещение матчей, а также карманников воров и поднадзорных лиц²⁰.

Количество камер видеонаблюдения, в том числе оснащенных технологиями ИИ, в России стремительно растет. Так, в 2023 г. количество систем видеонаблюдения увеличилось на 12 %. По итогам 2024 г. прогнозируется рост еще на 11 %. По количеству камер видеонаблюдения Российская Федерация находится на третьем месте после Китая и США. Большая часть камер с технологией ИИ используется для фиксации нарушений Правил дорожного движения (ПДД). Количество таких камер к концу 2023 г. составило 22 183, еще 909 камер планировалось установить в 2024 г.²¹ В 2023 г. с помощью камер фотовидеофиксации за нарушение ПДД было вынесено 220,9 млн постановлений на сумму около 140,9 млрд руб.²²

5. Заключение

Подводя итог, отметим, что в настоящее время технологии ИИ широко применяются для контроля над поведением населения во всех странах мира, где имеются соответствующие технологии. В том числе эта деятельность осуществляется и в целях охраны общественного порядка и борьбы с преступностью.

средств для обеспечения функций оперативно-розыскных мероприятий на сетях электросвязи Российской Федерации» // СвязьИнформ. 1999. № 6.

¹⁷ Постановление Европейского Суда по правам человека от 4 декабря 2015 г. по делу «Роман Захаров (Roman Zakharov) против Российской Федерации» (жалоба № 47143/06) // Бюллетень Европейского Суда по правам человека: рос. изд. М., 2016. № 6 (168).

¹⁸ Вестник Мэра и Правительства Москвы. 2012. № 8.

¹⁹ Городская система видеонаблюдения // Портал правительства Москвы. URL: <https://video.dit.mos.ru/> (дата обращения: 11.12.2024).

²⁰ Сайт компании NTECHLAB. URL: <https://ntechlab.ru/solution/public-safety/> (дата обращения: 11.12.2024).

²¹ Кодачигов В. Не первый взгляд: в РФ резко вырастет количество «штрафных» камер // Известия. 2024. 7 мая. URL: <https://iz.ru/1692531/valerii-kodachigov/ne-pervyi-vzgliad-v-rf-rezko-vyrastet-kolichestvo-shtrafnykh-kamer>.

²² В РФ в 2023 году штрафы по камерам за нарушения ПДД составили рекордную за пять лет сумму // ТАСС. 2024. 23 февр. URL: <https://tass.ru/obschestvo/20064853>.

Анализ восточного и западного подходов к правовому регулированию отношений, связанных с использованием ИИ в правоохране, позволяет сделать вывод о том, что возрастает актуальность проблемы обеспечения и защиты прав граждан в процессе сбора информации о них, ее обработки и принятия на этой основе решения компетентными органами и должностными лицами, поскольку данные решения могут являться причиной ограничения прав и свобод граждан, в том числе в связи с привлечением их к юридической ответственности.

Так, в Китае в настоящее время для «неблагонадежных» лиц введен ряд ограничений, связанных, например, с их передвижением (использование самолетов и поездов), родом занятий (запрет занимать руководящие должности в определенных сферах), получением финансовых услуг (отказ в выдаче кредитов) и др. [23, с. 23–24; 24, с. 748]. А в США такие лица без суда помещаются в тайные тюрьмы, где к ним применяются пытки [25; 26].

С учетом того, что правильность формулируемых ИИ выводов обусловлена компетентностью разработчиков алгоритмов и лиц, осуществляющих его обучение, расширение сферы применения ИИ, наделение его дополнительными полномочиями, в том числе по принятию юридически значимых решений, требует создания дополнительных гарантий защиты прав граждан в случаях совершения ошибки указанными специалистами. Учет данного обстоятельства предполагает создание в Российской Федерации механизма обжалования решений, принимаемых на основе данных ИИ (либо непосредственно ИИ) путем разработки правовых норм, его закрепляющих, и нацеливает на разработку теоретических представлений о наиболее рациональных формах и методах правового регулирования в рассматриваемой сфере общественной практики.

СПИСОК ЛИТЕРАТУРЫ

1. Науменко Т. В. Китайская система социального кредита: антиутопия или фактор общественного благополучия? / Т. В. Науменко, К. Н. Секретарева // Журнал исследований социальной политики. – 2022. – Т. 20, № 3. – С. 419–432. – DOI: 10.17323/727-0634-2022-20-3-419-432.
2. Плотников В. А. Цифровизация как закономерный этап эволюции экономической системы / В. А. Плотников // Экономическое возрождение России. – 2020. – № 2 (64). – С. 104–115. – DOI: 10.37930/1990-9780-2020-2-64-104-115.
3. Пролубников А. В. Платформенная модель государственной экономической политики / А. В. Пролубников // Многоуровневое общественное воспроизводство: вопросы теории и практики : сб. науч. тр. – Иваново, 2020. – Вып. 18 (34). – С. 21–34.
4. Швецов А. Н. Цифровизация госуправления в России на фоне лучшего зарубежного опыта / А. Н. Швецов, В. Н. Рысина // ЭКО. – 2020. – Т. 50, № 2. – С. 60–80. – DOI: 10.30680/ECO0131-7652-2020-2-60-80.
5. Vertakova Y. V. Synergy of Blockchain Technologies and “Big Data” in Business Process Management of Economic Systems / Y. V. Vertakova, T. A. Golovina, A. V. Polyanin // Digital Economy: Complexity and Variety vs. Rationality (ISC 2019) / eds. E. Popkova, B. Sergi. – Cham : Springer, 2020. – P. 856–865. – (Lecture Notes in Networks and Systems; vol. 87). – DOI: 10.1007/978-3-030-29586-8_97.
6. von Blomberg M. The Social Credit System and China’s rule of law / M. von Blomberg // Mapping China Journal. – 2018. – No. 2. – P. 77–112.
7. Гончаров В. В. Система социального доверия (социального рейтинга) в КНР: проблемы и перспективы внедрения в Российской Федерации / В. В. Гончаров, Е. Г. Петренко, А. А. Борисова, Л. В. Толмачева, И. А. Дмитриева // Административное и муниципальное право. – 2023. – № 3. – С. 78–91. – DOI: 10.7256/2454-0595.2023.3.39983.
8. Катрашова Ю. В. Система социального рейтинга как форма государственного контроля над обществом: перспективы внедрения и развития, угрозы реализации / Ю. В. Катрашова, Г. Ю. Митяшин, В. А. Плотников // Управленческое консультирование. – 2021. – № 2. – С. 100–109. – DOI: 10.22394/1726-1139-2021-2-100-109.
9. Creemers R. Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century / R. Creemers // Journal of Contemporary China. – 2017. – Vol. 26, No. 103. – P. 85–100. – DOI: 10.1080/10670564.2016.1206281.

10. Creemers R. China's Social Credit System: An Evolving Practice of Control / R. Creemers. – May 9, 2018. – 32 p. – DOI: 10.2139/ssrn.3175792.
11. Попов Д. И. План строительства системы социального кредита как дорожная карта реформы социального управления в Китае в 2010-х гг. / Д. И. Попов // Вестник Омского университета. Серия «Исторические науки». – 2020. – Т. 7, № 1. – С. 147–157. – DOI: 10.24147/2312-1300.2020.7(1).147-157.
12. Петров А. А. Информационно-цифровой след: коммерческие и социальные аспекты в цифровую эпоху / А. А. Петров // Торговая политика. – 2020. – № 2 (22). – С. 62–86. – DOI: 10.17323/2499-9415-2020-2-22-62-86.
13. Петров А. А. Китайский цифровой профиль или скоринговая система социального доверия / А. А. Петров // Chronos. – 2020. – № 8 (46). – С. 11–24.
14. Климонович А. П. Влияние цифровых технологий на современное общество. Пример системы рейтинга социального кредита в Китае / А. П. Климонович // Цифровая социология. – 2020. – Т. 3, № 3. – С. 35–44. – DOI: 10.26425/2658-347X-2020-3-3-35-44.
15. Разумов Е. А. Новые тенденции в системе социального рейтинга и информационной безопасности КНР в условиях обострения эпидемиологической ситуации / Е. А. Разумов // Вестник Дальневосточного отделения Российской академии наук. – 2021. – № 1. – С. 132–135. – DOI: 10.37102/0869-7698_2021_215_01_15.
16. Буяров Д. В. Система социального кредита в Синьцзян-Уйгурском автономном районе Китая / Д. В. Буяров // Genesis: исторические исследования. – 2024. – № 4. – С. 99–108. – DOI: 10.25136/2409-868X.2024.4.70522.
17. Антончева О. А. Влияние системы социального кредита в Китае на политическую коммуникацию / О. А. Антончева, Т. Е. Апанасенко // Управленческое консультирование. – 2022. – № 10. – С. 12–27. – DOI: 10.22394/1726-1139-2022-10-12-27.
18. Голубев С. Г. Система общественного доверия как инструмент управления цифровым обществом: китайский опыт / С. Г. Голубев, В. К. Сугак // Журнал Белорусского государственного университета. Социология. – 2019. – № 4. – С. 62–74.
19. Степанов О. А. Правовое регулирование генезиса цифровой личности / О. А. Степанов, М. М. Степанов // Правоприменение. – 2022. – Т. 6, № 3. – С. 19–32. – DOI: 10.52468/2542-1514.2022.6(3).19-32.
20. Степанов О. А. О правовом реагировании на последствия поведения личности в виртуальном пространстве / О. А. Степанов, М. М. Степанов // Правоприменение. – 2024. – Т. 8, № 1. – С. 24–33. – DOI: 10.52468/2542-1514.2024.8(1).24-33.
21. Степанов О. А. О цифровой идентификации действий личности / О. А. Степанов, М. М. Степанов // Государство и право. – 2024. – № 7. – С. 205–210. – DOI: 10.31857/S1026945224070185. – (На англ. яз.).
22. Piza E. CCTV Surveillance for Crime Prevention: A 40-Year Systematic Review with Meta-Analysis / E. Piza, B. Welsh, D. Farrington, A. Thomas // Criminology & Public Policy. – 2019. – Vol. 18, no. 1. – Р. 135–159.
23. Антропов Р. В. Система социального рейтинга в Китае: прогрессивный механизм поощрения и наказания или цифровая диктатура? / Р. В. Антропов, И. И. Лиценберг // Актуальные проблемы развития КНР в процессе ее регионализации и глобализации : материалы XII Междунар. науч.-практ. конф. – Чита : Забайк. гос. ун-т, 2020. – С. 20–27.
24. Петров А. А. Китайская система социальной оценки и электронные механизмы контроля / А. А. Петров // Большая Евразия: Развитие, безопасность, сотрудничество : ежегодник : материалы Третьей междунар. науч.-практ. конф. – М., 2020. – С. 737–756.
25. Глазунова Е. Н. Гуантанамо: история с продолжением / Е. Н. Глазунова // Вестник Московского университета. Серия 25: Международные отношения и мировая политика. – 2011. – № 3. – С. 153–183.
26. Крючков К. С. Отчет Хофмана: психологи и пытки. Этический урок для психологов / К. С. Крючков // Консультативная психология и психотерапия. – 2020. – Т. 28, № 1. – С. 148–165. – DOI: 10.17759/cpp.2020280109.

REFERENCES

1. Naumenko T., Sekretareva K. China's Social Credit System: Dystopia or Public Welfare Factor?. *Zhurnal issledovanii sotsial'noi politiki = The Journal of Social Policy Studies*, 2022, vol. 20, no. 3, pp. 419–432. DOI: 10.17323/727-0634-2022-20-3-419-432. (In Russ.).
2. Plotnikov V.A. Digitization as a logical stage in the evolution of an economic system. *Ekonomicheskoe vozrozhdenie Rossii = Economic Revival of Russia*, 2020, no. 2 (64), pp. 104–115. DOI: 10.37930/1990-9780-2020-2-64-104-115. (In Russ.).
3. Prolubnikov A.V. Platform model of state economic policy, in: *Mnogourovnevoe obshchestvennoe vospriyvostvo: voprosy teorii i praktiki*, collection of scientific papers, Ivanovo, 2020, iss. 18 (34), pp. 21–34. (In Russ.).
4. Shvetsov A.N., Rysina V.N. "Digitalization" of public management in Russia against the background of best international practice. *ECO*, 2020, vol. 50, no. 2, pp. 60–80. DOI: 10.30680/ECO0131-7652-2020-2-60-80. (In Russ.).
5. Vertakova Y.V., Golovina T.A., Polyanin A.V. Synergy of Blockchain Technologies and "Big Data" in Business Process Management of Economic Systems, in: Popkova E., Sergi B. (eds.). *Digital Economy: Complexity and Variety vs. Rationality (ISC 2019)*, Lecture Notes in Networks and Systems; vol. 87, Cham, Springer Publ., 2020, pp. 856–865. DOI: 10.1007/978-3-030-29586-8_97.
6. von Blomberg M. The Social Credit System and China's rule of law. *Mapping China Journal*, 2018, no. 2, pp. 78–112.
7. Goncharov V.V., Petrenko E.G., Borisova A.A., Tolmacheva L.V., Dmitrieva I.A. The system of social trust (social rating) in China: problems and prospects of implementation in the Russian Federation. *Administrativnoe i munitsipal'noe pravo = Administrative and municipal law*, 2023, no. 3, pp. 78–91. DOI: 10.7256/2454-0595.2023.3.39983. (In Russ.).
8. Katrashova Yu.V., Mityashin G.Yu., Plotnikov V.A. Social Rating System as a Form of State Control Over Society: Prospects for Implementation and Development, Threats to Realization. *Upravlencheskoe konsul'tirovanie = Administrative Consulting*, 2021, no. 2, pp. 100–109. DOI: 10.22394/1726-1139-2021-2-100-109. (In Russ.).
9. Creemers R. Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century. *Journal of Contemporary China*, 2017, vol. 26, no. 103, pp. 85–100. DOI: 10.1080/10670564.2016.1206281.
10. Creemers R. *China's Social Credit System: An Evolving Practice of Control*. May 9, 2018. 32 p. DOI: 10.2139/ssrn.3175792.
11. Popov D.I. The Social Credit System Construction Plan as a Roadmap for Social Management Reform in China in the 2010s. *Vestnik Omskogo universiteta. Seriya "Istoricheskie nauki" = Herald of Omsk University. Series "Historical Studies"*, 2020, vol. 7, no. 1, pp. 147–157. DOI: 10.24147/2312-1300.2020.7(1).147-157. (In Russ.).
12. Petrov A. Human digital informational footprint. *Torgovaya politika = Trade policy*, 2020, no. 2 (22), pp. 62–86. DOI: 10.17323/2499-9415-2020-2-22-62-86. (In Russ.).
13. Petrov A.A. Chinese Digital Profile or Social Trust Scoring System. *Chronos*, 2020, no. 8 (46), pp. 11–24. (In Russ.).
14. Klimovich A.P. The impact of digital technologies on modern society. An example of a social credit rating system in China. *Tsifrovaya sotsiologiya = Digital Sociology*, 2020, vol. 3, no. 3, pp. 35–44. DOI: 10.26425/2658-347X-2020-3-3-35-44. (In Russ.).
15. Razumov E.A. New trends in the system of social rating and information security of China in the face of escalation of epidemiological situation. *Vestnik Dal'nevostochnogo otdeleniya Rossiiskoi akademii nauk = Vestnik of the Far East Branch of the Russian Academy of Sciences*, 2021, no. 1, pp. 132–135. DOI: 10.37102/0869-7698_2021_215_01_15. (In Russ.).
16. Buyarov D.V. The social credit system in the Xinjiang Uygur Autonomous Region of China. *Genesis: istoricheskie issledovaniya*, 2024, no. 4, pp. 99–108. DOI: 10.25136/2409-868X.2024.4.70522. (In Russ.).
17. Antoncheva O.A., Apanasenko T.E. Impact of the Social Credit System in China on Political Communication. *Upravlencheskoe konsul'tirovanie = Administrative Consulting*, 2022, no. 10, pp. 12–27. DOI: 10.22394/1726-1139-2022-10-12-27. (In Russ.).
18. Golubev S.G., Suhak V.K. Chinese social credit system as the tool of governance in the digital era. *Zhurnal Belorusskogo gosudarstvennogo universiteta. Sotsiologiya = Journal of the Belarusian State University. Sociology*, 2019, no. 4, pp. 62–74. (In Russ.).

19. Stepanov O.A., Stepanov M.M. Legal regulation of the genesis of digital identity. *Pravoprimenenie = Law Enforcement Review*, 2022, vol. 6, no. 3, pp. 19–32. DOI: 10.52468/2542-1514.2022.6(3).19-32.
20. Stepanov O.A., Stepanov M.M. On the legal response to the consequences of personal behavior in virtual space. *Pravoprimenenie = Law Enforcement Review*, 2024, vol. 8, no. 1, pp. 24–33. DOI: 10.52468/2542-1514.2024.8(1).24-33.
21. Stepanov O.A., Stepanov M.M. On digital identification of actions personality. *Gosudarstvo i pravo = State and Law*, 2024, no. 7, pp. 205–210. DOI: 10.31857/S1026945224070185.
22. Piza E., Welsh B., Farrington D., Thomas A. CCTV Surveillance for Crime Prevention: A 40-Year Systematic Review with Meta-Analysis. *Criminology & Public Policy*, 2019, vol. 18, no. 1, pp. 135–159.
23. Antropov R.V., Litsenberg I.I. The China's social system: the progressive mechanism of reward and punishment or digital dictatorship?, in: *Aktual'nye problemy razvitiya KNR v protsesse ee regionalizatsii i globalizatsii*, Proceedings of the 12th International scientific and practical conference, Chita, Transbaikal State University Publ., 2020, pp. 20–27. (In Russ.).
24. Petrov A.A. Chinese social evaluation system and electronic monitoring mechanisms, in: *Bol'shaya Evraziya: Razvitie, bezopasnost', sotrudничество*, Annual, Proceedings of the Third international scientific and practical conference, Moscow, 2020, pp. 737–756. (In Russ.).
25. Glazunova E.N. Guantanamo: a story to be continued. *Vestnik Moskovskogo universiteta. Seriya 25: Mezhdunarodnye otnosheniya i mirovaya politika = Lomonosov World Politics Journal*, 2011, no. 3, pp. 153–183. (In Russ.).
26. Kryuchkov K.S. The Hoffman Report: Psychologists and Torture. An Ethical Precaution for Psychologists. *Konsul'tativnaya psikhologiya i psikhoterapiya = Counseling Psychology and Psychotherapy*, 2020, vol. 28, no. 1, pp. 148–165. DOI: 10.17759/cpp.2020280109.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Степанов Олег Анатольевич – доктор юридических наук, профессор, главный научный сотрудник центра судебного права
Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации
117218, Россия, г. Москва, ул. Б. Черемушкинская, 34
E-mail: soa-45@mail.ru
ORCID: 0000-0003-1103-580x
ResearcherID: O-9771-2019
Scopus AuthorID: 57208665632
SPIN-код РИНЦ: 8156-9725; AuthorID: 655914

Степанов Михаил Михайлович – кандидат юридических наук, доцент, ведущий научный сотрудник отдела теории права и междисциплинарных исследований законодательства
Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации
117218, Россия, г. Москва, ул. Б. Черемушкинская, 34
E-mail: stepanovtao@mail.ru
ORCID: 0000-0002-5203-1867
ResearcherID: AAX-2549-2020
Scopus AuthorID: 57215415345
SPIN-код РИНЦ: 2134-8209

INFORMATION ABOUT AUTHORS

Oleg A. Stepanov – Doctor of Law, Professor; Chief Researcher, Centre of Judicial Law
Institute of Legislation and Comparative Law under the Government of the Russian Federation
34, B. Cheremushkinskaya ul., Moscow, 117218, Russia
E-mail: soa-45@mail.ru
ORCID: 0000-0003-1103-580x
ResearcherID: O-9771-2019
Scopus AuthorID: 57208665632
RSCI SPIN-code: 8156-9725; AuthorID: 655914

Mikhail M. Stepanov – PhD in Law, Associate Professor; Leading Researcher, Department of Theory of Law and Interdisciplinary Research of Legislation
Institute of Legislation and Comparative Law under the Government of the Russian Federation
34, B. Cheremushkinskaya ul., Moscow, 117218, Russia
E-mail: stepanovtao@mail.ru
ORCID: 0000-0002-5203-1867
ResearcherID: AAX-2549-2020
Scopus AuthorID: 57215415345
RSCI SPIN-code: 2134-8209

БИБЛИОГРАФИЧЕСКОЕ ОПИСАНИЕ СТАТЬИ

Степанов О.А. Подходы к правовому регулированию отношений, связанных с использованием искусственного интеллекта в правоохране / О.А. Степанов, М.М. Степанов // Правоприменение. – 2025. – Т. 9, № 4. – С. 15–25. – DOI: 10.52468/2542-1514.2025.9(4).15-25.

BIBLIOGRAPHIC DESCRIPTION

Stepanov O.A., Stepanov M.M. Approaches to the legal regulation of artificial intelligence application in law enforcement. *Pravoprimenenie = Law Enforcement Review*, 2025, vol. 9, no. 4, pp. 15–25. DOI: 10.52468/2542-1514.2025.9(4).15-25. (In Russ.).