

Научная статья

УДК 347.1

DOI 10.25205/2542-0410-2023-19-3-69-77

## Проблемы защиты персональных данных в России и Китае: сравнительно-правовой анализ

Надежда Юльевна Чернусь<sup>1,2</sup>  
Сунь Юйпэн<sup>2</sup>

<sup>1</sup>Институт философии и права СО РАН  
Новосибирск, Россия

<sup>2</sup>Новосибирский национальный исследовательский государственный университет  
Новосибирск, Россия

<sup>1</sup>[preiudicia@yandex.ru](mailto:preiudicia@yandex.ru), <https://orcid.org/0000-0001-9316-524X>  
<sup>2</sup>[syp19960420@163.com](mailto:syp19960420@163.com), <https://orcid.org/0009-0001-6052-9825>

### Аннотация

В статье анализируется законодательство о персональных данных России и Китая, судебная практика КНР о защите персональной информации. Продемонстрировано, что законодательство России и КНР закрепляет понятие персональных данных, содержит принципы и механизм защиты персональных данных граждан, предусматривает меры ответственности за нарушение прав граждан при незаконном использовании их персональных данных. Рассмотренные примеры судебной практики КНР демонстрируют применение законодательства о персональных данных, привлечение нарушителей к гражданско-правовой, уголовной и административной ответственности. Формулируется вывод о том, что развитие интернет-технологий, технологий искусственного интеллекта, глубокого синтеза порождает множество проблем, связанных с незаконным использованием личной информации о гражданах, что требует постоянного совершенствования законодательства о защите персональных данных.

### Ключевые слова

персональные данные, защита персональных данных. способы защиты персональных данных. технологии искусственного интеллекта, технологии глубокого синтеза

### Для цитирования

Чернусь Н. Ю., Сунь Юйпэн. Проблемы защиты персональных данных в России и Китае: сравнительно-правовой анализ // Юридическая наука и практика. 2023. Т. 19, № 3. С. 69–77. DOI 10.25205/2542-0410-2023-19-3-69-77

## Problems of Personal Data Protection in Russia and China: Comparative Legal Analysis

Nadezhda Yu. Chernus<sup>1</sup>, Sun Yupeng<sup>2</sup>

<sup>1</sup>Federal State Budgetary Institution of Science, Institute of Philosophy and Law  
of the Siberian Branch of the Russian Academy of Sciences

<sup>2</sup>Novosibirsk National Research State University

<sup>1</sup>preiudicia@yandex.ru, <https://orcid.org/0000-0001-9316-524X>

<sup>2</sup>syp19960420@163.com, <https://orcid.org/0009-0001-6052-9825>

### Abstract

The article analyzes the legislation on personal data of Russia and China, the judicial practice of the People's Republic of China on the protection of personal information. It is demonstrated that the legislation of Russia and the People's Republic of China enshrines the concept of personal data, contains the principles and mechanism of protection of personal data of citizens, provides for liability measures for violation of the rights of citizens in the illegal use of their personal data. The considered examples of judicial practice of the People's Republic of China demonstrate the application of legislation on personal data, bringing violators to civil, criminal and administrative responsibility. The conclusion is formulated that the development of Internet technologies, artificial intelligence technologies, deep synthesis generates a lot of problems related to the illegal use of personal information about citizens, which requires constant improvement of legislation on personal data protection.

### Keywords

personal data; personal data protection, methods of personal data protection, artificial intelligence technologies, deep synthesis technologies

### For citation

Chernus N. Yu., Sun Yupeng. Problems of personal data protection in Russia and China: Comparative legal Analysis. *Juridical Science and Practice*, 2023, vol. 19, no. 3, pp. 69–77. (in Russ.) DOI 10.25205/2542-0410-2023-19-3-69-77

Одним из приоритетных направлений развития науки, технологий и техники в Российской Федерации является развитие информационно-телекоммуникационных систем<sup>1</sup>. В связи с появлением технологии искусственного интеллекта современное развитие информационных систем зависит от внедрения технологий, направленных на более совершенное функционирование любой системы, для работы которой необходимо постоянное принятие интеллектуальных, творческих решений. В целях обеспечения ускоренного развития искусственного интеллекта в Российской Федерации, проведения научных исследований в области искусственного интеллекта, повышения доступности информации и вычислительных ресурсов для пользователей, совершенствования системы подготовки кадров в этой области Президентом РФ утверждена Национальная стратегия развития искусственного интеллекта на период до 2030 года<sup>2</sup>.

Поскольку ключевым элементом технологии искусственного интеллекта являются большие массивы данных (big data), для некоторых сфер деятельности (например, медицины) такие базы формируются из персональной информации, получение и обработка которой требует соблюдения прав обладателей этой информации. В процессе получения и обработки таких персональных данных существует угроза нарушения прав и свобод граждан, что обуславливает необходимость закрепления в законодательстве понятного и эффективного механизма защиты персональных данных граждан.

<sup>1</sup> См.: Указ Президента РФ от 7 июля 2011 г. № 899 «Об утверждении приоритетных направлений развития науки, технологий и техники в Российской Федерации и перечня критических технологий Российской Федерации» // Собрание законодательства РФ. 2011. № 28. Ст. 4168.

<sup>2</sup> Указ Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» // Официальный интернет-портал правовой информации <http://www.pravo.gov.ru>, 11 октября 2019 г.

В России в настоящее время действует Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»<sup>3</sup> (далее – Закон о персональных данных), который регулирует отношения, связанные с обработкой персональных данных с целью обеспечения защиты прав и свобод человека и гражданина, в том числе для защиты прав на неприкосновенность частной жизни, личной и семейной тайны. Тем не менее процесс формирования информационного общества происходит такими темпами, когда при выборе между внедрением новой технологии, использующей персональные данные, и соблюдением прав и свобод гражданина выбор делается в пользу технологий. Согласие гражданина на обработку его персональных данных приобретает формальный смысл, когда без этого согласия гражданин просто лишается возможности оперативно получить необходимую услугу. Между тем использование персональных данных приобретателями может иметь самые неблагоприятные последствия для субъекта персональных данных. Несмотря на наличие правового регулирования процессов обработки и использования персональных данных, в настоящее время до сих пор отсутствуют общие принципы обращения информации в цифровом пространстве, поскольку приоритеты между правами и свободами гражданина (защита персональных данных) и товаром (коммерческое использование персональных данных) не расставлены окончательно.

Проблема усугубляется отсутствием единого подхода к пониманию персональной информации, общего механизма ее защиты. Закон о персональных данных содержит широкое определение персональных данных, под которыми понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст. 3 Закона о персональных данных). Такое определение позволяет в различных нормативно-правовых актах использовать разные подходы к пониманию персональной информации, что позволяет придавать персональной информации отраслевую природу, когда правовое регулирование и защита персональных данных будет зависеть от характера правоотношений, в рамках которого произошло правонарушение. Например, Постановлением Правительства РФ от 30.06.2018 № 772<sup>4</sup> определен состав сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, включая вид биометрических персональных данных. Данное Постановление (которое не утратило силу) было принято в соответствии с уже утратившей силу ч. 8 ст. 14.1 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»<sup>5</sup> – обстоятельство, которое подтверждает отсутствие единой системы правового регулирования обработки и защиты персональной информации.

Несмотря на недостатки правового регулирования, Конституция РФ гарантирует каждому право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Также каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения (ст. 23 Конституции РФ). Иными словами, информация, содержащая персональные данные субъекта персональных данных, должна иметь гарантированный уровень правовой и организационно-технической защиты.

Обратимся к законодательству Китайской Народной Республики, где в августе 2019 года в целях обеспечения безопасности личной информации о несовершеннолетних были изданы «Правила защиты персональных данных детей в Сети»<sup>6</sup>. В сентябре 2019 года для пресече-

<sup>3</sup> Рос. газета. 2006. 29 июля.

<sup>4</sup> Официальный интернет-портал правовой информации <http://www.pravo.gov.ru>, 03.07.2018.

<sup>5</sup> Рос. газета. 2006. 29 июля.

<sup>6</sup> Правила защиты персональных данных детей в Сети // База данных национальных законов и нормативных актов. URL: <https://flk.npc.gov.cn/> (дата обращения: 01.08.2023).

ния незаконного использования приложений, собирающих личную информацию граждан, Национальная администрация киберпространства Китая обнародовала «Методы выявления незаконного сбора и использования личной информации приложениями», которые позволяют выявить незаконное использование приложений, содержащих личную информацию граждан<sup>7</sup>. В январе 2020 года вступил в силу Гражданский кодекс КНР (далее – ГК КНР), согласно которому персональные данные физических лиц охраняются законом (ст. 1034)<sup>8</sup>. Соответственно при нарушении законодательства о персональных данных граждан неправомерными действиями могут быть использованы общеправовые способы защиты, предусмотренные гражданским законодательством для защиты личных неимущественных прав. В ноябре 2021 года в Китае принят Закон КНР «О защите личной информации»<sup>9</sup> (далее – Закон о защите личной информации), содержащий целую систему гарантий защиты личной информации граждан. Согласно ст. 4 Закона, к личной информации относятся все виды информации, относящейся к идентифицированным или идентифицируемым физическим лицам, записанной в электронном или ином виде, за исключением анонимной информации.

Анализ Закона о защите личной информации позволяет сформулировать несколько его ключевых положений. Во-первых, Закон определяет личную информацию как такую информацию, которая не только позволяет идентифицировать определенное лицо, но и, что наиболее важно, это информация, которая также может быть использована для идентификации конкретного человека. Во-вторых, источник, в котором может содержаться личная информация, является практически любым, т. е. информация «записывается в электронном виде или иными способами». В-третьих, понятие «идентифицируемый» по отношению к обладателю персональных данных означает, что соответствующая информация не всегда может идентифицировать конкретное физическое лицо. Персональные данные могут быть объединены с информацией из другого источника или нуждаться в ином преобразовании для идентификации конкретного физического лица. Фактически лицо может быть идентифицировано при условии совершения дополнительных действий с соответствующей информацией, касающейся этого лица. В-четвертых, персональные данные принадлежат только физическим лицам, исключая юридических лиц и иные объединения. При этом физические лица могут распоряжаться своей личной информацией, в том числе посредством завещания. В-пятых, анонимизация относится к технической обработке персональных данных, при которой субъект персональных данных не может быть идентифицирован или ассоциирован, а обработанная информация не может быть восстановлена. Хотя в настоящее время полная «анонимизация» с помощью современных технологий невозможна.

С принятием в КНР Закона о защите личной информации последовало дальнейшее правовое регулирование сбора и обработки персональных данных. Так, в декабре 2021 г. Национальное сетевое информационное управление Китая приняло Положения об объеме необходимой личной информации для распространенных типов мобильных интернет-приложений<sup>10</sup>, где «общая личная информация» граждан разделена на 39 категорий, а при ее незаконном использовании любая организация или физическое лицо, обнаружившие нарушения этих правил,

<sup>7</sup> Методы выявления незаконного сбора и использования личной информации приложениями // База данных национальных законов и нормативных актов. URL: <https://flk.npc.gov.cn/> (дата обращения: 01.08.2023).

<sup>8</sup> Гражданский кодекс Китайской Народной Республики // База данных национальных законов и нормативных актов. URL: <https://flk.npc.gov.cn/> (дата обращения: 01.08.2023).

<sup>9</sup> Закон о защите личной информации Китайской Народной Республики (от 20 августа 2021 года) // База данных национальных законов и нормативных актов. URL: <https://flk.npc.gov.cn/> (дата обращения: 01.08.2023).

<sup>10</sup> Положения об объеме необходимой личной информации для распространенных типов мобильных интернет-приложений. URL: [http://www.cac.gov.cn/2021-03/22/c\\_1617990997054277.htm/](http://www.cac.gov.cn/2021-03/22/c_1617990997054277.htm/) (дата обращения: 01.08.2023).

могут сообщить об этом в соответствующий отдел (ст. 6 Положений). Кроме того, местные законодательные органы Китая также имеют собственное законодательство о персональных данных. В частности, в 2022 г. вступило в силу Положение о данных Шэньчжэньской особой экономической зоны<sup>11</sup>, которое является типичным примером местного законодательства Китая о персональных данных.

В настоящее время помимо Закона о защите личной информации в КНР действуют Закон об электронной подписи Китайской Народной Республики<sup>12</sup>, Закон о безопасности данных Китайской Народной Республики<sup>13</sup>, Закон о кибербезопасности Китайской Народной Республики<sup>14</sup> и другие нормативно-правовые акты, которые составляют основу законодательства о персональных данных Китая.

Множество нормативно-правовых актов, принятых в КНР, направленных на защиту личной информации граждан, позволяет сформулировать принципы правовой охраны персональных данных гражданина.

Первый принцип *информированного согласия* заключается в том, что перед обработкой персональных данных гражданина операторы обработки данных уведомляют этого гражданина на указанными в законе способами и получают письменное согласие гражданина на это (либо фиксируют это согласие в форме электронных документов). В данном случае гражданин имеет право отказаться, и персональные данные гражданина не подлежат обработке. Так, согласно п. 3 ст. 24 Закона о защите личной информации, при принятии решений, оказывающих существенное влияние на права и интересы личности путем автоматизированного принятия решений, физические лица имеют право потребовать, чтобы обработчик личной информации объяснил, и имеют право отказать обработчику личной информации в принятии решений только посредством автоматизированного принятия решений. Аналогичный принцип содержится и в российском законодательстве, когда обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных (п. 1 ч. 1 ст. 6 Закона о персональных данных), возможность отказа от автоматизированной обработки его персональных данных закреплена в ч. 3 ст. 16 Закона о персональных данных.

Следующий принцип *необходимого объема обрабатываемых персональных данных* выражается в том, что объем обрабатываемых персональных данных должен соответствовать цели обработки этих персональных данных. Кроме того, оператор должен выбрать такой способ обработки персональных данных, который позволит обеспечить максимальную защиту личных прав и законных интересов субъектов персональных данных. Статья 5 Закона о персональных данных также содержит указанный принцип, включающий сразу несколько похожих положений. Во-первых, обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных. Во-вторых, не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, не совместимых между собой. В-третьих, обработке подлежат только персональные данные, которые отвечают целям их обработки. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их

<sup>11</sup> Портал законов Китая CJO. URL: <https://ru.chinajusticeobserver.com/law/x/data-regulation-of-the-shenzhen-special-economic-zone20210629> (дата обращения: 01.08.2023).

<sup>12</sup> Закон об электронной подписи // База данных национальных законов и нормативных актов. URL: <https://flk.npc.gov.cn/> (дата обращения: 01.08.2023).

<sup>13</sup> Закон о безопасности данных Китайской Народной Республики от 10 июня 2021 года // База данных национальных законов и нормативных актов. URL: <https://flk.npc.gov.cn/> (дата обращения: 01.08.2023).

<sup>14</sup> Закон о кибербезопасности Китайской Народной Республики от 01 июня 2017 года // База данных национальных законов и нормативных актов. URL: <https://flk.npc.gov.cn/> (дата обращения: 01.08.2023).



обработки. Наконец, при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

Следующий принцип – *отраслевого характера отношений по обработке персональных данных*. В данном случае, поскольку цели обработки персональных данных могут быть различными, начиная от автоматизированной обработки персональных данных мобильными операторами, заканчивая персонифицированным учетом, осуществляемым в отношении граждан органами публичной власти, здесь персональные данные могут быть классифицированы в зависимости от характера персональных данных на персональные данные, содержащие: личную конфиденциальную информацию, общедоступную личную информацию, биометрические данные, корпоративную информацию, финансовую информацию и др. В Российской Федерации также в различных правовых отраслях приняты положения, учитывающие особенности правоотношений, возникающих в процессе обработки персональных данных<sup>15</sup>.

Приведенные принципы правовой охраны персональных данных обуславливают наличие целой системы мер защиты персональных данных в России и КНР. Можно выделить общие и специальные способы защиты персональных данных граждан.

Общие способы защиты гражданских прав содержатся в ст. 12 Гражданского кодекса РФ (далее – ГК РФ)<sup>16</sup>. Для защиты нарушенных прав, связанных с незаконной обработкой и распространением персональных данных, могут быть применены такие способы, как: восстановление положения, существовавшего до нарушения права, и пресечения действий, нарушающих право или создающих угрозу его нарушения; самозащита права; возмещение убытков; компенсация морального вреда; прекращение или изменения правоотношения; иные способы, предусмотренные законом. В ГК КНР также содержатся способы защиты гражданских прав, среди которых для защиты права на личную информацию можно выделить: пресечение действий, нарушающих закон или создающих угрозу его нарушения (ст. 997 ГК КНР); возмещение убытков (ст. 1182 ГК КНР); восстановление репутации и принесение извинения (ст. 995 ГК КНР); компенсация морального вреда (ст. 996 ГК КНР).

В качестве примера защиты прав на личную информацию можно привести дело, рассмотренное Высшим народным судом провинции Шаньдун (дело № (2020)浙0192民初10605号)<sup>17</sup>. Ответчик разместил два последовательных сообщений на Weibo, раскрывающих имя Чжана (истца), дату рождения, номер телефона, место жительства, место работы и другую личную информацию. После того как истец узнал об этом, он позвонил в полицию, и ответчик удалил личную информацию об истце, но продолжал размещать личную информацию против истца на Weibo. Согласно решению суда, ответчик обязан принести извинения, компенсировать моральный вред и убытки.

<sup>15</sup> См., например: глава 14 Трудового кодекса Российской Федерации от 30 декабря 2001 г. № 197-ФЗ; глава 7 Федерального закона от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации»; ст. 84 части первой Налогового кодекса Российской Федерации от 31 июля 1998 г. № 146-ФЗ.

<sup>16</sup> Часть первая Гражданского кодекса Российской Федерации от 30 ноября 1994 г. № 51-ФЗ // Собрание законодательства Российской Федерации. 1994. № 32. Ст. 3301.

<sup>17</sup> В связи с конфиденциальной информацией данное судебное решение не было опубликовано, дело находится в ведении Высшего народного суда провинции Шаньдун. См: Шаньдунский высший народный суд 鲁司法案例[2023]071 // Официальный сайт Высшего народного суда провинции Шаньдун. URL: [sdcourt.gov.cn](http://sdcourt.gov.cn) (дата обращения: 01.08.2023).

В Уголовном кодексе КНР<sup>18</sup> последствиями совершения преступления, связанного с нарушением права на охрану персональных данных граждан, являются штраф и тюремное заключение (ст. 253.1 – Преступление, связанное с нарушением персональных данных граждан; ст. 286.1 – Преступление, заключающееся в отказе выполнять обязательства по управлению безопасностью информационной сети).

Согласно материалам уголовного дела, рассмотренного судом г. Ханчжоу (дело 鲁司法案例 [2023]071)<sup>19</sup>, подсудимый приобрел персональные данные граждан у других лиц через свою группу QQ (известный интернет-чат в Китае) и перевел их на свой аккаунт Baidu в облачный диск. В то же время данные неоднократно перепродавались другим лицам, и неоднократно взимались сборы на общую сумму 49 600 юаней. Согласно судебному решению, подсудимый совершил преступление, заключающееся в нарушении персональных данных граждан, и был приговорен к трем годам тюремного заключения и штрафу в размере 10 000 юаней.

Среди специальных способов защиты прав субъектов персональных данных законодательство КНР предусматривает, прежде всего, ответственность, предусмотренную главой 7 Закона о защите личной информации. Так, в соответствии со ст. 66 Закона, в случае обработки персональных данных с нарушением положений настоящего Закона или без выполнения обязательств по защите персональных данных, предусмотренных настоящим Законом, органы, отвечающие за защиту персональных данных, должны предписать нарушителю внести исправления, вынести предупреждение, конфисковать незаконные доходы, а также распорядиться о приостановке или прекращении предоставления услуг приложениями, которые неправомерно обрабатывают личную информацию; если нарушитель отказывается внести исправления, на него налагается штраф в размере не более одного миллиона юаней; и ответственные лица с прямой ответственностью и другие лица с прямой ответственностью должны быть оштрафованы на сумму не менее 10,000 100,000 юаней каждое.

В качестве примера применения специальных мер защиты прав субъектов персональных данных можно привести дело, рассмотренное судом Ханчжоу (дело № (2020) 浙0192民初10993号)<sup>20</sup>. Ответчик без информирования и получения согласия субъекта персональных данных зарегистрировал учетную запись с целью сбора и хранения личной информации о несовершеннолетнем лице, включая его местоположение, контактную информацию и конфиденциальные персональные данные, такие как информация о заболеваниях, изображение, голос и другие характеристики ребенка. На основании решения суда ответчик компенсировал 1,5 миллиона юаней за ущерб, причиненный правам и охраняемым законом интересам несовершеннолетнего.

Российское законодательство о персональных данных не содержит специальных способов защиты прав физических лиц, если произошло соответствующее правонарушение. Согласно ст. 24 Закона о персональных данных, лица, виновные в нарушении требований настоящего Федерального закона, несут предусмотренную законодательством Российской Федерации ответственность. Таким образом, нарушители несут гражданско-правовую, дисциплинарную, административную и уголовную ответственность в соответствии с положениями соответствующего законодательства. Так, гражданско-правовая ответственность за нарушение личных неимущественных прав предусмотрена общими положениями ГК РФ (ст. 12, 152.2 ГК РФ), административная ответственность предусмотрена Кодексом Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ<sup>21</sup> (ст. 13.11 предусматривает ответственность за нарушение законодательства Российской Федерации в области персональ-

<sup>18</sup> Портал законов Китая CJO. URL: <https://ru.chinajusticeobserver.com/law/x/criminal-law-of-china-20171104> (дата обращения: 01.08.2023).

<sup>19</sup> Постановление Интернет-суда Ханчжоу от 11.03.2021 г. (2020) 浙0192民初10993号 // China Judgements Online. URL: <https://wenshu.court.gov.cn/> (дата обращения: 01.08.2023).

<sup>20</sup> Там же.

<sup>21</sup> Рос. газета. 2001. 31 дек.

ных данных). За разглашение персональных данных одного работника другим, если эти данные стали известны в связи с исполнением трудовых обязанностей, наступает ответственность в виде расторжения трудового договора по инициативе работодателя (подп. «в» п. 6 ч. 1 ст. 81 Трудового кодекса РФ от 30 декабря 2001 г. № 197-ФЗ<sup>22</sup>).

На основании проведенного сравнительного анализа законодательства и правоприменительной практики о персональных данных России и Китая следует прийти к выводу, что правовая система Китая в сфере защиты персональных данных содержит более эффективный механизм защиты прав граждан на личную информацию, особенно в условиях цифровизации гражданского оборота, и способствует дальнейшему развитию и совершенствованию правового регулирования отношений, возникающих в информационном (цифровом) пространстве. Развитие интернет-технологий, технологий искусственного интеллекта, глубокого синтеза порождает множество проблем, связанных с незаконным использованием личной информации о гражданах, что требует постоянного совершенствования законодательства о защите персональных данных. Уже в настоящее время широкое применение технологий глубокого синтеза требует обеспечения защиты прав граждан, чьи персональные данные могут быть незаконно использованы с целью причинения вреда этим гражданам, поскольку использование технологий глубокого синтеза позволяет, изменяя внешность и голос, вводить в заблуждение на видео и иных изображениях, нарушать права граждан на личную информацию, честь, достоинство, деловую репутацию и изображение. Технология глубокого синтеза может использоваться с целью нарушения прав граждан в киберпространстве: мошенничества, незаконных переводов денежных средств с личных счетов граждан и др. В КНР действует специальное законодательство, регулирующее использование технологии глубокого синтеза. Так, согласно ст. 23 Положения об администрировании глубокого синтеза информационных сервисов Интернета, технология глубокого синтеза относится к технологии использования глубокого обучения, виртуальной реальности и других синтетических алгоритмов для создания текста, изображений, аудио, видео, виртуальных сцен и другой сетевой информации<sup>23</sup>. В КНР уже начинает складываться судебная практика по делам о нарушении прав при использовании технологии глубокого синтеза. Приведем в качестве примера дело, рассмотренное судом г. Чэнду (дело № (2022) 川|7101民初6349号)<sup>24</sup>, в котором ответчик нарушил права истца, используя программное обеспечение для изменения лица на своем мобильном телефоне. Суд принял решение, согласно которому ответчик обязан немедленно удалить видео, нарушающее авторские права истца, отключить ссылку и прекратить дальнейшее нарушение прав истца на изображение.

Итак, цифровизация гражданского оборота, появление новых технологий требуют совершенствования законодательства о персональных данных. Наличие новых типов персональной информации, включая биометрические данные, появление технологий алгоритмического использования персональных данных порождают множество правовых проблем, решение которых возможно путем принятия специального законодательства о защите личных прав граждан в информационном пространстве. Специальное законодательство должно учесть изменившуюся форму общественных отношений, установить ответственность отдельных субъектов, операторов, использующих современные технологии при обработке персональных данных физических лиц.

<sup>22</sup> Рос. газета. 2001. 31 дек.

<sup>23</sup> Положение об администрировании глубокого синтеза информационных сервисов Интернета от 25 ноября 2022 г. // База данных национальных законов и нормативных актов URL: <https://flk.npc.gov.cn/> (дата обращения: 01.08.2023).

<sup>24</sup> Постановление Первого железнодорожного транспортного суда Чэнду от 04.08.2022 г. (2022) 川|7101民初6349号 // China Judgements Online. URL: <https://wenshu.court.gov.cn/> (дата обращения: 01.08.2023).



### **Информация об авторах**

**Надежда Юльевна Чернусь**, кандидат юридических наук

**Сунь Юйпэн**, аспирант

### **Information about the authors**

**Nadezhda Yu. Chernus**, Candidate of Law Sciences

**Sun Yupeng**, Postgraduate Student

*Статья поступила в редакцию 20.07.2023;  
одобрена после рецензирования 21.07.2023; принята к публикации 31.07.2023*  
*The article was submitted 20.07.2023;  
approved after reviewing 21.07.2023; accepted for publication 31.07.2023*