УДК 34.09
DOI 10.52468/2542-1514.2022.6(3).120-133

ЦИФРОВЫЕ ИННОВАЦИИ И ПРАВА ЧЕЛОВЕКА: ДИЛЕММЫ МЕЖДУНАРОДНОЙ ПРАВООХРАНИТЕЛЬНОЙ ПРАКТИКИ

М.А. Михайлов, Т.А. Кокодей
Севастопольский государственный университет, г. Севастополь, Россия

Информация о статье
Дата поступления –
14 февраля 2022 г.
Дата принятия в печать –
20 июня 2022 г.
Дата онлайн-размещения –
20 сентября 2022 г.

Ключевые слова
Цифровизация, информационно-коммуникационные тренды, защита, персональные данные, цифровые технологии, международная правоохранительная практика, идентификация, биометрические данные

Предпринимается попытка проведения сравнительного анализа правового регулирования защиты персональных данных в четырех странах: Китае, Беларуси, США и России – и формулирования соответствующих рекомендаций в контексте глобальных информационно-коммуникационных трендов. Рассматриваются существующие в настоящее время противоречия между возможностями, предоставляемыми инновационными цифровыми технологиями идентификации физических лиц и обработки их персональных данных, с одной стороны, и правами человека – с другой. Делаются выводы относительно необходимых в настоящее время изменений законодательства Российской Федерации по защите персональных данных с учетом технологических возможностей.

DIGITAL INNOVATION AND HUMAN RIGHTS: DILEMMAS IN INTERNATIONAL LAW ENFORCEMENT PRACTICE

Mikhail A. Mikhailov, Tatiana A. Kokodey
Sevastopol State University, Sevastopol, Russia

Article info
Received –
2022 February 14
Accepted –
2022 June 20
Available online –
2022 September 20

Keywords
Digitalization, information and communication trends, protection, personal data, digital technologies, international law enforcement practice, identification, biometric data

The subject of the study is the legal nature of personal data, as well as a set of legal norms governing relations in the field of their processing and circulation in the Russian Federation and foreign countries. The article uses a comparative method, a system analysis method, as well as a forecasting method.
The purpose of the article is to confirm or refute the hypotheses about the further strengthening of the contradictions between the emergence and implementation of new technologies for processing personal data versus ensuring the protection of human rights, as well as the expediency and possibility of using foreign legislative experience in domestic practice to counter these threats and reduce the risks arising from this and damage.
Main results, scope. The article examines the legislative experience of legal regulation of the types, scope, and nature of personal data in the People's Republic of China, the United States of America, the Republic of Belarus, and the Russian Federation. At the same time, Chinese legislation most quickly responds to the challenges of the criminal use of biometric technologies, American legal norms are less acceptable for our practice due to the peculiarities of case law, and Belarusian law has only recently entered into force, opening the era of legal regulation in this area. The facts of the use of new technologies (such as deepfake) for the processing of biometric information for criminal purposes and the problems of law enforcement in this area, as well as legal disputes of citizens who have suffered damage from the use of these technologies, are analyzed. It is predicted that it will be impossible to fully ensure the protection of human rights in the context of the emergence of new technologies for processing personal data. The importance of the desire to predict threats to the protection of personal information at the stage of emergence of new technologies for processing personal data in order to neutralize them in a timely manner is indicated.

ISSN 2658-4050 (Online)

Conclusion. An analysis of the legislation of foreign countries will make it possible to give preference to the Chinese experience, which promptly counteracts the risks of using new technologies for criminal purposes. An analysis of domestic and global law enforcement practice will make it possible to predict the spread of new ways of committing crimes, the misuse of personal data, and vulnerabilities in their storage and protection. At the same time, excessive restrictions on access to data, their processing and their circulation can make it difficult for law enforcement agencies to solve the tasks of ensuring state security and the protection of public order. It requires constant monitoring of threats and risks and timely technical and legal response to their manifestation. The purpose of the study has been achieved, ways to improve legislation in order to protect human rights in the context of the introduction of digital innovations in all spheres of human activity are proposed. Security, combating crime.

1. Введение

Научно-технический прогресс, коснувшийся всех сфер человеческой деятельности, стал причиной противоречий, которые еще несколько лет назад не вызывали особой озабоченности у общества и государства. Речь идет об обороте персональных данных человека, их объеме и характере, сборе, хранении, распространении и необходимости защиты в условиях проявления цифровых инновационных методов их обработки.

Современные технологии позволяют генерировать, получать, хранить и обрабатывать значительные объемы такой информации, отслеживая, таким образом, все обстоятельства, из которых складывается поведение и состояние конкретного человека, а также анализировать законопослушность и моральные качества, прогнозировать дальнейшие поступки. С развитием глобальной сети «Интернет» такая информация оказалась в бесконтрольном доступе и попадает в распоряжение злоумышленников.

Таким образом, благие цели внедрения этих технологий были дискредитированы рисками нарушения права человека на неприкосновенность частной жизни, что замедлило их реализацию. В то же время противодействие преступности, а прежде всего такому опасному его проявлению, как терроризм, не позволяет игнорировать эффективные цифровые инструменты для выявления и нейтрализации преступников, минимизации причиняемого ими ущерба.

Проблема противоречия распространения современных информационно-коммуникационных технологий требованиям соблюдения прав человека достаточно недавно стала объектом внимания отечественных авторов, прежде всего из области информационного и конституционного права, а также уголовного, административного и гражданского права. В частности, Е.В. Виноградова, Т.А. Полякова и А.В. Минбалеев, А.Н. Мочалов, В.В. Блажеев, М.А. Егорова, Э.В. Талапина, А.К. Жарова рассматривают феномен цифрового профиля и правовое регулирование отношений в сфере цифрового профилирования [1–6]. Правовому регулированию искусственного интеллекта в целом посвящены работы В.Б. Наумова и К.Ю. Никольской [7–9].

Отдельные аспекты проблемы рассматриваются и в публикациях таких специалистов уголовного процесса и криминалистики, как А.Ф. Волынский, Н.В. Максимов и К.В. Бугаев [10–12]. Правовые аспекты использования систем идентификации субъекта путем электронного распознавания лица и этические проблемы дактилоскопической регистрации населения рассматривались и одним из авторов настоящей статьи [13–15]. Во многом усугублению рассматриваемой проблемы способствовала глобальная пандемия *COVID*-19 [16–19].

Необходимость законодательного регулирования определения объема и характера персональных данных, механизмов их защиты при получении, обработке и обороте по-разному реализована в отдельных странах мира в зависимости от вида правовой системы, уровня развития информационных технологий, оперативности законодательного реагирования. Последнее особенно важно не только для уже получивших значительное распространение методов, например геномной регистрации [20], но и в условиях появления новых технологий, связанных с распознаванием голоса, фото- и видеоизображения внешности [21–24].

Другими инновационными технологиями биометрической аутенфикации являются сочетание таких биометрических модальностей, как пальцевые узоры и электроэнцефалограмма [25; 26], а также идентификация по радужной оболочке и сетчатке глаза [27; 28] и клавиатурному почерку [29; 30].

Представленный выше законодательный опыт подлежит тщательному изучению с целью учета ошибок и успехов, предотвращения рисков в отечественной практике и прогнозирования их дальней-

шего развития с одновременным соблюдением конституционных требований охраны прав человека.

2. Правовое регулирование защиты персональных данных в Китае

Начало 2022 г. положило конец неконтролируемому получению информации из баз данных в стране с активно формирующимся законодательством по защите персональных данных вследствие вступления в силу Закона от 1 ноября 2021 г. «О защите персональной информации» (*Personal Information Protection Law*; далее – Закон КНР)[1]. Данный закон расширил требования предыдущего, акцентируя внимание на защите информации, позволяющей идентифицировать личность гражданина Китая. Как указано в ст. 1, миссией закона является «защита прав и интересов индивидов», «регулирование обработки персональных данных» и «обеспечение разумного использования персональной информации». При этом законодатель не распространяет действие закона на жителей Гонконга, Макао и Тайваня[2].

По мнению экспертов, закон позволит защитить рядовых граждан и оптимизировать регулирование интернет-экономики, охраняя интересы интернет-пользователей путем устранения нарушений, вызванных неконтролируемым сбором личной информации, в том числе и личных персональных и биометрических данных пользователей.

Так, в последние годы большое развитие получают технологии распознавания лиц. Начиналось это в частных компаниях и в коммерческих целях. Большинство компаний, управляющих недвижимостью в Китае, стали требовать от собственников и жильцов помещений прохождения обязательного биометрического сканирования при входе в жилые комплексы. Затем повсеместное распространение этой практики привело к тому, что появились первые судебные иски, например в 2021 г. Гу Бин стал первым в Китае истцом, предъявившим требование за применение технологии распознавания лиц к зоопарку.

Еще в начале пандемии *COVID*-19 для борьбы с ней во многих общественных местах была внедрена эта технология, она снизила нагрузку на охрану, в том числе и по термометрии клиентов. Однако основной причиной, вызвавшей повсеместное использование технологий идентификации личности, является возможность извлечения сверхприбылей путем ее применения для целенаправленного маркетингового воздействия на конкретных клиентов.

В этих целях китайский производитель электромобилей *XPeng Motors* нелегально собрал 430 000 изображений лиц посетителей его магазинов за шесть месяцев, но впоследствии был принужден удалить эту базу. Население также считает, что такие технологии должны применяться лишь органами охраны порядка и спецслужбами, а не частными организациями.

Несмотря на то, что в мире подобные технологии находят всё большее развитие и распространение, в большинстве стран отсутствует не только правовое регулирование такой деятельности, но и государственная политика в этой сфере.

На данный момент назрела необходимость в установлении определенного баланса между внедрением этих технологий, которые безусловно полезны, особенно в сферах борьбы с преступностью, охраны общественного порядка, государственной безопасности, и мерами по защите персональных данных, охраны прав и свобод человека. Проблема из этической для большинства государств мира давно переросла в правовую.

Ответом Китая на этот вызов и стал Закон КНР – первый законодательный акт страны, в котором сделан акцент на систематизацию мер по защите личной информации граждан. Он выверен в соответствии с принципом информированного согласия, т. е. в качестве основного правила защиты личной информации дает гражданам право знать и право принимать решения в отношении своей личной информации.

При комплексном применении данного закона, Закона «О кибербезопасности» (*Cyber Security Law*) и Закона «О безопасности данных» (*Data Security Law*) создается всеобъемлющая правовая база защиты информации, соблюдения требований к корпоративным данным и цифровой экономике Китая.

Статья 4 Закона КНР дает определение понятия персональных данных как всех видов информации, записанных электронными или иными средствами, относящихся к идентифицированным или идентифицируемым физическим лицам, не включая при этом информацию, полученную после обработки анонимизированных данных.

[1] Liu Caiyu, Zhang Dan. Excessive data mining to come to an end as China's personal info protection law comes into effect // Global Times. 01 Nov. 2021. URL: https://www.globaltimes.cn/page/202111/1237844.shtml. См. также: [31; 32].

[2] The national people's congress of the People's republic of China. URL: http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml.

ISSN 2658-4050 (Online)

Обработка персональных данных включает в себя сбор, хранение, использование, обработку, передачу, предоставление, раскрытие, удаление личной информации.

Закон КНР запрещает чрезмерный сбор личной информации (ст. 6) и ценовую дискриминацию с использованием больших баз данных в отношении клиентов. При бизнес-маркетинге для отдельных лиц путем автоматизированного принятия решений обработчики персональной информации должны предоставлять варианты, которые не нацелены на личные характеристики, или предлагать методы отказа.

При обращении с личной информацией должны соблюдаться принципы открытости и прозрачности, раскрытия правил обращения с личной информацией и четкое указание цели, способа и объема обработки.

В ст. 13 Закона КНР перечислены условия, позволяющие обрабатывать личную информацию без согласия субъекта:

– при заключении и выполнении договоров, в котором физическое лицо является заинтересованной стороной, в том числе и трудовых;

– при необходимости в целях выполнения уставных обязанностей и привлечения к ответственности за их нарушение;

– при необходимости реагировать на внезапные угрозы в области общественного здравоохранения или защищать жизнь и здоровье физических лиц или сохранность их имущества в чрезвычайных условиях;

– в разумных пределах для подачи новостей, наблюдения за общественным мнением и иных подобных действий в общественных интересах;

– при обработке личной информации, раскрытой самими лицами или иным образом уже раскрытой на законных основаниях, в разумных пределах в соответствии с положениями настоящего закона;

– при обстоятельствах, предусмотренных иными законами и подзаконными актами.

Требуемое согласие пользователей должно быть получено для обработки онлайн-сервисами такой личной информации, как биометрические, медицинские данные, данные о здоровье, финансовых счетах и местоположении.

Закон КНР также требует приостановки или прекращения предоставления услуг для приложений, которые незаконно обрабатывают персональные данные. При этом необходимо учитывать, что в Китае сегодня около 1 млрд интернет-пользователей, более 4 млн веб-сайтов и 3 млн приложений.

Закон КНР требует, чтобы интернет-гиганты, владеющие личной информацией большого числа пользователей, создавали независимые структуры, в основном из внешних наблюдателей, контролирующие обработку информации.

По мере реализации Закона КНР предприниматели, акционеры и инвесторы крупных китайских технологических компаний должны понимать, что «золотая эра» получения солидной прибыли за счет вторжения в частную жизнь пользователей и чрезмерного сбора данных осталась в прошлом. Использование персональных данных должно соответствовать мировым стандартам.

Согласно ст. 26 Закона КНР установка оборудования для сбора изображений или распознавания личности в общественных местах должна осуществляться в соответствии с требованиями обеспечения общественной безопасности и соблюдения соответствующих государственных постановлений, также должны устанавливаться четкие указывающие на это знаки. Собранные личные изображения и личная отличительная идентификационная информация могут использоваться только в целях защиты общественной безопасности; они не могут использоваться для других целей, за исключением случаев, когда получено отдельное согласие отдельных лиц.

В Законе КНР также введено понятие конфиденциальных персональных данных (ст. 28). Это личная информация, которая в случае утечки или незаконного использования может причинить вред чести и достоинству физического лица либо существенный вред личной или имущественной безопасности, включая сведения о биометрических характеристиках, религиозных убеждениях, особом статусе, здоровье, финансовых счетах, индивидуальном местоположении и т. д., а также личная информация несовершеннолетних в возрасте до 14 лет. Только при наличии конкретной цели и необходимости, а также при условии строгих мер защиты разрешено обрабатывать конфиденциальные персональные данные, для чего следует получить отдельное согласие физического лица.

Введение вышеуказанных законодательных требований уже в начале 2022 г. привело к возникновению противоречий между развитием инновационных цифровых технологий в стране и правовыми

ограничениями на их использование[3]. Администрация управления киберпространством (*The Cyberspace Administration of China*) – центральный орган регулирования Интернета Китая – в настоящее время рассматривает введение правил использования технологии глубокого синтеза (*The deep synthesis technology*) для защиты законных прав и интересов граждан в стране в рамках правового акта – Положения об администрировании глубокого синтеза информационных сервисов Интернета (*Internet Information Service Deep Synthesis Management Provisions*; далее – Положение)[4]. Глубокий синтез – это типичное применение технологии искусственного интеллекта. В прошлом данная технология была известна как дипфейк (*deepfake*), потому что ее можно было использовать для создания несуществующего видео- и аудиоконтента, что создает потенциальные проблемы для охраны общественного порядка, борьбы с преступностью и национальной безопасности. Тем не менее у рассматриваемой технологии есть и множество общественно полезных применений в таких сферах, как кино- и телепроизводство, помощь пациентам с нарушением речи. Думается, именно поэтому более приемлем нейтральный термин «глубокий синтез».

В ст. 2 Положения перечисляются сферы применения этой технологии:

1. Технологии генерации или редактирования текстового контента (генерация текста, трансформация стиля письма, диалоги в форме вопросов и ответов).

2. Технологии создания или редактирования голосового контента (преобразование текста в речь, преобразование голоса и редактирование характеристик голоса).

3. Технологии создания или редактирования неголосового звукового контента (создание музыки и редактирование звуков окружающей среды).

4. Технологии создания или редактирования лица человека на изображениях или видео (создание лиц, замена лиц, редактирование черт внешности, изменение мимики и телодвижений).

5. Технологии редактирования небиологических характеристик изображений или видео (улучшение и восстановление изображения).

6. Технологии создания или редактирования виртуальных настроек (трансформация двухмерных моделей в трехмерные).

В марте 2021 г. органы госрегулирования Китая потребовали от 11 влиятельных китайских интернет-компаний, в числе которых были *Tencent*, *Xiaomi* и *Kuaishou*, усилить оценку безопасности голосового программного обеспечения и новых интернет-технологий и приложений, использующих технологию глубокого синтеза дипфейк.

Последним небезопасным ее проявлением стало приложение *Avatarify*, в котором используется искусственный интеллект, позволяющий пользователю заменять свои собственные лица лицами других людей при создании фото- и видеопродукции. По сообщениям СМИ, приложение стало очень распространенным (вирусным) на сервисе для просмотра коротких видео *TikTok* в феврале 2021 г. и уже было загружено более 1,5 млн раз. Однако по требованию властей 2 марта приложение было удалено из китайского магазина приложений *Apple* ввиду опасений по поводу вторжения в частную жизнь.

В марте 2021 г. полиция г. Чжэнчжоу (Центральный Китай) предупредила, что использование программного обеспечения для изменения лица сопряжено с определенными рисками безопасности, такими как утечка личной информации, и что такие технологии часто используются в преступных целях, а созданные после этого видеоролики зачастую являются порнографией. Это еще одна причина усиления защиты персональных данных в Китае.

В ст. 6 Положения вводится новое понятие «портретные права»: ни одна организация или физическое лицо не может использовать услуги «глубокого синтеза» (*deep synthesis*) для участия в деятельности, которая нарушает права других людей на защиту от неправомерного использования их изображений, защиту репутации, на неприкосновенность частной жизни, портретные права и другой контент, охраняемый законом.

Статья 9 Положения предписывает поставщикам услуг технологии «глубокого синтеза» проводить аутентификацию реальной идентификационной информации пользователей их сервиса и запрещает публиковать эту информацию.

[3] China mulls regulations for deep synthesis technology // Global Times. 28 Jan. 2022. URL: https://www.globaltimes.cn/page/202201/1250193.shtml.

[4] Internet Information Service Deep Synthesis Management Provisions (Draft for Comment). Jan. 2022. URL: https://digichina.stanford.edu/work/translation-internet-information-service-deep-synthesis-management-provisions-draft-for-comment-jan-2022/.

ISSN 2658-4050 (Online)

В тех случаях, когда поставщик услуг «глубокого синтеза» предлагает функции, включающие в себя существенную обработку биометрической информации, такой как лицо и человеческий голос, перед редактированием информации пользователю услуги следует получить индивидуальное согласие субъекта на редактируемую личную информацию, за исключением случаев, предусмотренных законодательством и административными регламентами.

Таким образом, цель документа – направить эту технологию на путь здорового развития, предотвратить риски и повысить ее положительную роль в техническом отношении.

3. Механизмы регулирования отношений в сфере защиты персональных данных в Беларуси

Законодательное закрепление регулирования персональных данных в Беларуси реализовано в основных положениях Закона Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» (далее – Закон РБ), вступившего в силу 15 ноября 2021 г. после его пятилетней разработки. До введения данного закона Беларусь оставалась одной из последних стран в мире, где практически не существовало защиты персональных данных. Основным инструментом, призванным содействовать выполнению операторами положений вышеуказанного закона, является комплекс прав физических лиц как субъектов персональных данных, позволяющий им контролировать и влиять на процесс обработки личной информации.

Что касается понятия персональных данных, в рамках Закона РБ предусмотрена их широкая трактовка, предполагающая включение в них *IP* и *email*-адресов физических лиц. То есть, согласно ст. 1, персональные данные – это любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано. Дополнительно данной статьей вводятся понятия:

– генетические персональные данные – информация, относимая к наследуемым либо приобретенным генетическим характеристикам человека, которая содержит уникальные данные о его физиологии либо здоровье и может быть выявлена, в частности, при исследовании его биологического образца;

– специальные персональные данные – персональные данные, касающиеся расовой либо национальной принадлежности, политических взглядов, членства в профессиональных союзах, религиозных или других убеждений, здоровья или половой жизни, привлечения к административной или уголовной ответственности, а также биометрические и генетические персональные данные;

– обработка персональных данных – любое действие или совокупность действий, совершаемые с персональными данными, включая сбор, систематизацию, хранение, изменение, использование, обезличивание, блокирование, распространение, предоставление, удаление.

Обработку персональных данных регламентирует гл. 2 Закона РБ. Обработка персональных данных осуществляется с согласия субъекта персональных данных, за исключением случаев, предусмотренных данным законом и иными законодательными актами. В целом согласие на обработку персональных данных по закону имеет три свойства: информированность, свободность и конкретность.

Статья 6 Закона РБ определяет условия, при которых обработка персональных данных может осуществляться без согласия физического лица, в том числе согласия на обработку персональных данных (исключая специальные персональные данные) не требуется:

– для целей ведения административного и (или) уголовного процесса, осуществления оперативно-разыскной деятельности;

– для осуществления правосудия, исполнения судебных постановлений и иных исполнительных документов;

– в целях осуществления контроля (надзора) в соответствии с законодательными актами;

– при реализации норм законодательства в области национальной безопасности, борьбы с коррупцией, предотвращения легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения;

– для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных или иных лиц, если получение согласия субъекта персональных данных невозможно, др.

Статья 8 Закона РБ определяет порядок обработки специальных персональных данных, в том числе условия, при которых не требуется согласие физического лица:

– при обработке общественными объединениями, политическими партиями, профессиональными союзами, религиозными организациями персональных данных их учредителей (членов) для достижения уставных целей при условии, что эти данные не подлежат распространению без согласия субъекта персональных данных;

– в целях организации оказания медицинской помощи при условии, что такие персональные данные обрабатываются медицинским, фармацевтическим или иным работником здравоохранения, на которого возложены обязанности по обеспечению защиты персональных данных и в соответствии с законодательством распространяется обязанность сохранять врачебную тайну;

– для осуществления правосудия, исполнения судебных постановлений и иных исполнительных документов, совершения исполнительной надписи, оформления наследственных прав;

– для целей ведения административного и (или) уголовного процесса, осуществления оперативно-разыскной деятельности;

– в целях обеспечения функционирования единой государственной системы регистрации и учета правонарушений;

– в целях ведения криминалистических учетов;

– в случаях, предусмотренных уголовно-исполнительным законодательством, законодательством в области национальной безопасности, об обороне, о борьбе с коррупцией, о борьбе с терроризмом и противодействии экстремизму, о предотвращении легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения, др.

В соответствии с гл. 4 Закона РБ был также создан уполномоченный орган по защите прав субъектов персональных данных – Национальный центр защиты персональных данных Республики Беларусь (https://cpd.by), – к основным функциям которого можно отнести: контроль за обработкой персональных данных операторами, рассмотрение жалоб субъектов персональных данных по вопросам обработки персональных данных, подготовку проектов актов законодательства о персональных данных, др.

4. Правоохранительные практики в сфере защиты персональных данных в США

Национальная правовая система США, функционирующая на принципах англосаксонской правовой семьи, не предусматривает каких-либо федеральных правовых актов по защите персональных данных, в отличие от большинства ведущих стран мира. При нарушении данных прав в основном применяют практику прецедентного права, а также положения Конституции США.

Основными действующими нормативно-правовыми актами в сфере обработки персональных данных являются законы о конфиденциальности (*Privacy Act*, 1974) и о защите частной жизни (*Privacy Protection Act*, 1980), которые регулируют деятельность органов государственной власти в этой области.

Закон о конфиденциальности 1974 г. защищает личную информацию, находящуюся в распоряжении федерального правительства, путем предотвращения несанкционированного ее распространения. Физические лица также имеют право на получение данных сведений, а также вправе быть информированными об их изменениях и передаче таких сведений кому-либо.

Очевидно, что вышеуказанные нормативные акты, принятые около полувека назад, не в полной мере отвечают требованиям современной цифровой эпохи и требуют кардинального обновления.

В 2010 г. Национальным институтом стандартов и технологий (*National Institute of Standards and Technology*, *NIST*) было разработано Руководство по защите конфиденциальности личной информации (*NIST Special Publication 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*)[5], целью которого стало правовое регулирование деятельности государственных органов и федеральных агентств по защите персональных данных граждан. Однако этот акт содержит лишь общие рекомендации по защите персональных данных без детализации механизма выполнения его требований, а также определения основных понятий.

В США под персональными данными понимается любая информация о физическом лице, хранимая агентством, включая (1) сведения, которые могут быть использованы для идентификации физического лица или слежки за ним, например имя, номер документа социального страхования, дата и место рождения, девичья фамилия матери или биометрические параметры, и (2) любые другие сведения, которые связаны или могут быть связаны с физическим лицом, например медицинская, образовательная, финансовая информация и информация о трудоустройстве.

Этот акт определяет принципы обращения с персональными данными, в числе которых:

– ограничение порядка получения этих данных, т. е. использование только законных способов для этого, а при необходимости и получение согласия

[5] URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf.

субъекта персональных данных на сбор такой информации;

– персональные данные должны по содержанию соответствовать целям, для достижения которых они будут использоваться; необходимо, чтобы они были точными, полными и регулярно обновляемыми;

– персональные данные не должны распространяться, передаваться кому-либо конкретно или иным образом использоваться для целей, отличных от заявленных, кроме как с согласия субъекта данных или в силу закона, др.

Это свидетельствует о том, что в США отсутствует единый механизм, регламентирующий обработку и защиту персональных данных.

При этом действующие правовые нормы содержат в основном определения соответствующих понятий и общие рекомендации, которые адресованы преимущественно государственным органам. В то же время текущего контроля над операторами персональных данных не ведется, а ответственность наступает лишь после утечки конфиденциальной информации. После выявления таких случаев нередко возникают проблемы с квалификацией преступления. Таким образом, персональная информация отдельных лиц очень уязвима.

Например, в марте 2021 г. жительница штата Пенсильвания Рафаэлла Споун (*Raffaela Spone*) обвинялась в использовании искаженных изображений и видео, созданных по технологии дипфейк, для дискредитации нескольких участников команды чирлидеров, которые составляли конкуренцию ее дочери. На сфальсифицированном контенте соперницы ее дочери предстали употребляющими алкоголь и курившими электронные сигареты. Обвинитель квалифицировал данные действия лишь как кибербуллинг именно из-за отсутствия достаточной правовой базы по защите персональных данных[6].

5. Сравнительный анализ правового регулирования защиты персональных данных в России и зарубежных странах

При разработке законодательства о персональных данных наша страна использовала ключевые принципы ведущих государств мира, учитывая ранее сформированные отечественные подходы к обеспечению информационной безопасности. Российская Федерация в области защиты персональных данных ратифицировала Конвенцию Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных» (ETS № 108, 1981 г.), в соответствии с которой в целях обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных был принят Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»[7] (далее – Закон РФ). Впоследствии были приняты федеральные законы о внесении изменений в Закон РФ от 25 июля 2011 г. № 261-ФЗ[8] и от 30 декабря 2020 г. № 519-ФЗ[9], при этом последние поправки вступили в силу с 1 марта 2021 г., ужесточив ответственность за утечку персональных данных

В Законе РФ под персональными данными в широком смысле понимается «любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)» (ч. 1 ст. 3).

При этом под обработкой персональных данных понимается «любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных» (п. 2 ст. 3).

В ст. 9 указано, что субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе.

Статья 11 Закона РФ определяет порядок использования биометрических персональных данных, под которыми понимаются «сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персо-

[6] Fitzsimons T. US News Pennsylvania cheer squad mom allegedly cyberbullied minors with deepfakes, officials say // NBC News. March 14, 2021. URL: https://www.nbcnews.com/news/us-news/pennsylvania-cheer-squad-mom-allegedly-cyberbullied-minors-deepfakes-officials-say-n1261055.

[7] Собрание законодательства Российской Федерации. 2006. № 31. Ст. 3451.

[8] Собрание законодательства Российской Федерации. 2011. № 31. Ст. 4701.

[9] Собрание законодательства Российской Федерации. 2021. № 1. Ст. 58.

нальных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных». Исключением, когда не требуется согласия субъекта, являются случаи, предусмотренные ч. 2 ст. 11: «в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию».

Сравнивая подходы к защите персональных данных в России и законодательствах других стран, рассмотренных выше, можно сделать следующие выводы:

1. В Российской Федерации существует единый механизм, включающий полномочия всех участников: операторов, субъектов и государственных уполномоченных органов, – при этом данный механизм основывается на условии обязательности защиты персональных данных. Российские нормативные документы регламентируют конкретные меры по защите персональных данных и ответственность за их утечку. Практически аналогичным является белорусское законодательство в данной области, которое фактически повторяет российские нормативные акты. Можно отметить, что законодательство обеих стран носит превентивный характер и направлено на упреждение нарушений.

2. В Соединенных Штатах Америки не существует единого механизма, который бы регламентировал обработку и защиту персональных данных, при этом нормативные акты носят характер общих рекомендаций. Также в США активно применяется практика прецедентного права, т. е. ответственность операторов наступает только после фактической утечки конфиденциальной информации, что препятствует формированию эффективной системы защиты частной информации граждан. Такой путь обеспечения защиты персональных данных кардинально отличается от пути большинства европейских стран.

3. Республика Беларусь еще только начинает ощущать последствия угроз в сфере защиты персональных данных и в то же время имеет свое видение к обеспечению права на неприкосновенность личной жизни. Однако ее опыт новичка в этой сфере, только формирующего законодательство, также может быть полезен для нашей страны, учитывая близость наших стран и менталитет народов.

4. Страной с наиболее активно развивающимися цифровыми технологиями и в связи с этим столь же стремительно формирующимся законодательством по защите персональных данных является Китайская Народная Республика. При этом ее первые законодательные и подзаконные акты по защите персональных данных по большей мере систематизируют общие рекомендации по защите личной информации и правила по использованию инновационных технологий для ее сбора и обработки. Это обстоятельство и должно послужить причиной пристального внимания отечественного законодателя к опыту этой страны как в связи с появлением новых угроз, вызванных развитием научно-технического прогресса, так и с успехами наших соседей в их нейтрализации и преодолении.

6. Заключение

Настоящее исследование направлено на решение актуальной проблемы обеспечения адекватной защиты персональных данных в России в условиях стремительной цифровизации всех сфер жизни общества, без ущемления прав человека на неприкосновенность личной жизни.

Основываясь на проведенном анализе, следует констатировать, что развитие информационно-коммуникационных технологий неминуемо приводит к ситуациям, угрожающим обеспечению прав человека. Ни технические, ни законодательные, ни этические препятствия не способны полностью устранить эту проблему.

С другой стороны, чрезмерные ограничения в получении, хранении и обработке этих данных судебными и правоохранительными органами могут существенного затруднить обеспечение государственной безопасности, противодействие преступности и таким ее опасным проявлениям, как терроризм, а также охрану общественного порядка.

Трудно объяснимы, сложно контролируемы, а значит, и неэффективны требования получения согласия от субъекта на обработку его персональных данных, в частности изображения лица, его голоса и т. п., которые он добровольно размещает в глобальной сети «Интернет» (в социальных сетях, на видеохостингах и т. п.).

Как и несколько лет назад при появлении цифровой фотографии, мы стоим на пороге очередного качественного скачка развития технологий, позволя-

ющих изменить виртуальные изображения человека, аудиограмму его голоса и подделать их под иное конкретное лицо. Это неминуемо приведет к появлению новых способов совершения правонарушений, к противодействию которым необходимо готовиться уже сейчас, как технически, так и законодательно.

Оперативный мониторинг правоприменительной практики, как отечественной, так и зарубежной, позволит если не исключить, то хотя бы минимизировать ущерб от таких проявлений. Изучение опыта законодателей зарубежных стран (прежде всего Китая) и его адаптация под отечественную специфику также будут способствовать решению этих задач.

Основными направлениями совершенствования отечественного законодательства в сфере защиты персональных данных следует считать:

– оперативную корректировку объема и вида персональных данных, требующих особой защиты;

– определение вида персональных данных, обработка которых возможна только с согласия самого субъекта;

– правовое реагирование на появление новых угроз в связи появлением ранее неизвестных технологий (на примере глобального синтеза биометрической информации лица – дипфейк);

– усиление и дифференциация гражданско-правовой, административной и уголовной ответственность за ненадлежащую защиту персональных данных, нарушение при этом прав человека.

Выражаем надежду, что тема соблюдения прав человека при использовании технологий обработки персональных данных будет в фокусе постоянного внимания специалистов в этой сфере, ученых и практиков, что позволит достаточно эффективно противодействовать преступным проявлениям в этой сфере.

СПИСОК ЛИТЕРАТУРЫ

1. Виноградова Е. В. Цифровой профиль: понятие, механизмы регулирования и проблемы реализации / Е. В. Виноградова, Т. А. Полякова, А. В. Минбалеев // Правоприменение. – 2021. – Т. 5, № 4. – С. 5–19. – DOI: 10.52468/2542-1514.2021.5(4).5-19.

2. Мочалов А. Н. Цифровой профиль: основные риски для конституционных прав человека в условиях правовой неопределенности / А. Н. Мочалов // Lex russica. – 2021. – Т. 74, № 9 (178). – С. 88–101. – DOI: 10.17803/1729-5920.2021.178.9.088-101.

3. Цифровое право : учеб. / под общ. ред. В. В. Блажеева, М. А. Егоровой. – М. : Проспект, 2020. – 640 с.

4. Механизмы и модели регулирования цифровых технологий : моногр. / под ред. А. В. Минбалеева. – М. : Проспект, 2020. – 264 с.

5. Талапина Э. В. Защита персональных данных в цифровую эпоху: Российское право в европейском контексте / Э. В. Талапина // Труды Института государства и права Российской академии наук. – 2018. – Т. 13, № 5. – С. 117–150.

6. Жарова А. К. Вопросы обеспечения безопасности цифрового профиля человека / А. К. Жарова // Юрист. – 2020. – № 3. – С. 55–61.

7. Nikolskaia K. Artificial Intelligence in Law / K. Nikolskaia, V. Naumov // 2020 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon). – Vladivostok, 2020. – P. 1–4. – DOI: 10.1109/FarEastCon50210.2020.9271095.

8. Nikolskaia K. Ethical and Legal Principles of Publishing Open Source Dual-Purpose Machine Learning Algorithms / K. Nikolskaia, V. Naumov // 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS). – Yaroslavl, 2020. – P. 56–58. – DOI: 10.1109/ITQMIS51053. 2020.9322897.

9. Правовые и этические аспекты, связанные с разработкой и применением систем искусственного интеллекта и робототехники: история, современное состояние и перспективы развития : моногр. / под общ. ред. канд. юрид. наук В. Б. Наумова. – СПб. : НП-Принт, 2020. – 258 с.

10. Волынский А. Ф. К вопросу о создании единой государственной системы регистрации граждан: проблемы, пути их решения / А. Ф. Волынский // Вестник Московского университета МВД России. – 2011. – № 9. – С. 56–58.

11. Максимов Н. В. Правовые вопросы дактилоскопирования гражданского населения / Н. В. Максимов // Казанские уголовно-процессуальные и криминалистические чтения : материалы Междунар. науч.-практ. конф. – Казань, 2022. – С. 193–196.

12. Бугаев К. В. Права человека и сроки хранения дактилоскопической информации: Российский опыт / К. В. Бугаев // Ученые записки Таврического национального университета имени В.И. Вернадского. Серия: Юридические науки. – 2008. – Т. 21, № 1 (60). – С. 211–216.

13. Михайлов М. А. Этические проблемы дактилоскопической регистрации населения / М. А. Михайлов // Совершенствование системы дактилоскопической регистрации : сб. материалов Междунар. науч.-практ. конф. (8 окт. 2015 г.). – М. : Юрлитинформ, 2016. – С. 153–160.

14. Михайлов М. А. Биометрия: Новое слово в идентификации личности / М. А. Михайлов // Воронежские криминалистические чтения : сб. науч. тр. / под ред. О. Я. Баева. – Воронеж : Изд-во Воронеж. гос. ун-та, 2009. – Вып ll. – С. 267–280.

15. Михайлов М. А. Правовые и этические аспекты распространения и использования систем идентификации человека путем электронного распознавания лица / М. А. Михайлов // Проблемы получения и использования доказательственной и криминалистически значимой информации : материалы Междунар. науч.-практ. конф. / отв. ред. М. А. Михайлов. – Симферополь : Ариал, 2019. – С. 79–82.

16. Williams C. C. The coronavirus pandemic and Europe's undeclared economy: impacts and a policy proposal / C. C. Williams, A. Kayaoglu // South East European Journal of Economics and Business. – 2020. – Vol. 15, iss. 1. – P. 80–92. – DOI: 10.2478/jeb-2020-0007.

17. Лунгу Е. В. Пандемия COVID-19. Новый вызов конституционным отношениям / Е. В. Лунгу // Правоприменение. – 2020. – Т. 4, № 3. – С. 69–75. – DOI: 10.24147/2542-1514.2020.4(3).69-75.

18. Правовое регулирование искусственного интеллекта в условиях пандемии и инфодемии / под общ. ред. проф. В. В. Блажеева, проф. М. А. Егоровой. – М. : Проспект, 2020. – 240 с.

19. Егорова М. А. Основные направления правового регулирования использования искусственного интеллекта в условиях пандемии / М. А. Егорова, А. В. Минбалеев, О. В. Кожевина, А. Дюфло // Вестник Санкт-Петербургского университета. Право. – 2021. – Т. 12, № 2. – С. 250–262. – DOI: 10.21638/spbu14.2021.201.

20. Анисимов В. А. Геномная регистрация всего населения и этические вопросы формирования и использования соответствующих баз данных / В. А. Анисимов, А. М. Сагитов, Э. К. Хуснутдинова, В. И. Луценко, А. В. Чемерис, Ф. Г. Аминев // Актуальные проблемы судебно-экспертной деятельности в уголовном, гражданском, арбитражном процессе и по делам об административных правонарушениях : материалы VII Междунар. науч.-практ. конф. 9 нояб. 2018 г. – Уфа : РИЦ БашГУ, 2018. – С. 16–22.

21. Матвеев Ю. Н. Технологии биометрической идентификации личности по голосу и другим модальностям / Ю. Н. Матвеев // Вестник Московского государственного технического университета им. Н.Э. Баумана. – 2012. – № 3 (3). – С. 5. – DOI: 10.18698/2308-6033-2012-3-91.

22. Westerlund M. The Emergence of Deepfake Technology: A Review // Technology innovation management review. – 2019. – Vol. 9, iss. 11, – P. 39–52.

23. Fitzgerald A. Our Deepfake Future // Virginia Quarterly Review. – 2020. – Vol. 96, no. 1. – P. 8–13.

24. Zendran M. Swapping Face Images with Generative Neural Networks for Deepfake Technology – Ex-perimental Study / M. Zendran, A. Rusiecki // Procedia computer science. – 2021. – Vol. 192. – P. 834–843.

25. Qunjian Wu. An EEG-Based Person Authentication System with Open-Set Capability Combining Eye Blinking Signals / Qunjian Wu, Ying Zeng, Chi Zhang, Li Tong, Bin Yan // Sensors (Basel). – 2018. – Vol. 18, iss. 2. – Art. 335. – DOI: 10.3390/s18020335.

26. Hui-Ling Chan. Challenges and Future Perspectives on Electroencephalogram-Based Biometrics in Person Recognition / Hui-Ling Chan, Po-Chih Kuo, Chia-Yi Cheng, Yong-Sheng Chen // Frontiers in Neuroinformatics. – 2018. – Vol. 12. – Art. 66. – DOI: 10.3389/fninf.2018.00066.

27. Ушмаев О. С. Биометрическая идентификация по радужной оболочке глаза: Текущее состояние и перспективы / О. С. Ушмаев // Графикон'2011 : 21-я междунар. конф. по компьютерной графике и машинному зрению. – М. : МАКС Пресс, 2011. – С. 192–194.

28. Барсуков С. С. Криминалистическая идентификация по радужной оболочке и сетчатке глаза: Современные возможности и проблемы применения / С. С. Барсуков // Юристъ-Правоведъ. – 2021. – № 1 (96). – С. 170–175.

29. Еременко Ю. И. Об идентификации клавиатурного почерка пользователей / Ю. И. Еременко, Ю. С. Олюнина // Перспективы развития информационных технологий. – 2016. – № 28. – С. 145–151.

30. Уварова А. В. Идентификация по клавиатурному почерку / А. В. Уварова, Е. А. Вещев // Интеграция науки и образования : сб. ст. по материалам междунар. науч.-практ. конф. – Иркутск : Апекс, 2017. – С. 27–30.

31. Разумов Е. А. Цифровое диктаторство: особенности системы социального кредита в КНР / Е. А. Разумов // Труды института истории, археологии и этнографии ДВО РАН. – 2019. – № 24. – С. 94–95.

32. Пинкевич Т. В. Нарушение неприкосновенности частной жизни при использовании технологии «больших данных» / Т. В. Пинкевич, А. В. Нестеренко // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2019. – № 3 (47). – С. 143–147.

REFERENCES

1. Vinogradova E.V., Polyakova T.A., Minbaleev A.V. Digital profile: concept, regulation mechanisms and implementation problems. *Pravoprimenenie = Law Enforcement Review*, 2021, Vol. 5, no. 4, pp. 5–19. DOI: 10.52468/2542-1514.2021.5(4).5-19. (In Russ.).

2. Mochalov A.N. Digital profile: main risks for constitutional human rights in the face of legal uncertainty. *Lex russica*, 2021, vol. 74, no. 9 (178), pp. 88–101. DOI: 10.17803/1729-5920.2021.178.9.088-101. (In Russ.).

3. Blazheev V.V., Egorova M. A. (eds.). *Digital law*, Textbook. Moscow, Prospekt Publ., 2020. 640 p. (In Russ.).

4. Minbaleev A.V. (ed.). *Mechanisms and models of regulation of digital technologies*, Monograph. Moscow, Prospekt Publ., 2020. 264 p.

5. Talapina E.V. Protection of personal data in the digital age: Russian law in the European context. *Trudy Instituta gosudarstva i prava Rossiiskoi akademii nauk = Proceedings of the Institute of State and Law of the Russian Academy of Sciences*, 2018, vol. 13, no. 5, pp. 117–150. (In Russ.).

6. Zharova A.K. Issues of ensuring the security of a person's digital profile. *Yurist = Lawyer*, 2020, no. 3, pp. 55–61. (In Russ.).

7. Nikolskaia K., Naumov V. Artificial Intelligence in Law, in: *2020 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon)*, Vladivostok, 2020, pp. 1–4. DOI: 10.1109/FarEastCon50210.2020.9271095.

8. Nikolskaia K., Naumov V. Ethical and Legal Principles of Publishing Open Source Dual-Purpose Machine Learning Algorithms, in: *2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*, Yaroslavl, 2020, pp. 56–58. DOI: 10.1109/ITQMIS51053. 2020.9322897.

9. Naumov V.B. (ed.). *Legal and ethical aspects related to the development and application of artificial intelligence systems and robotics: history, current state and development prospects*, Monograph. St. Petersburg, NP-Print Publ., 2020. 258 p. (In Russ.).

10. Volynsky A.F. On the issue of creating a unified state system for registering citizens: problems, ways to solve them. *Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia*, 2011, no. 9, pp. 56–58. (In Russ.).

11. Maksimov N.V. Legal issues of fingerprinting the civilian population, in: *Kazanskie ugolovno-protsessual'nye i kriminalisticheskie chteniya*, Materials of the International scientific-practical conference, Kazan, 2022, pp. 193–196. (In Russ.).

12. Bugaev K.V. Human rights and terms of storage of fingerprint information: Russian experience. *Uchenye zapiski Tavricheskogo natsional'nogo universiteta imeni V.I. Vernadskogo. Seriya: Yuridicheskie nauki = Scientific notes of the Taurida National University named after V.I. Vernadsky. Series: Legal Sciences*, 2008, vol. 21, no. 1 (60), pp. 211–216. (In Russ.).

13. Mikhailov M.A. Ethical problems of fingerprint registration of the population, in: *Sovershenstvovanie sistemy daktiloskopicheskoi registratsii*, a collection of materials of the International scientific and practical conferences (October 8, 2015), Moscow, Yurlitinform Publ., 2016, pp. 153–160. (In Russ.).

14. Mikhailov M.A. Biometrics: A new word in personal identification, in: Baev O.Ya. (ed.). *Voronezhskie kriminalisticheskie chteniya*, collection of scientific works, iss. ll, Voronezh, Voronezh State University Publ., 2009, pp. 267–280. (In Russ.).

15. Mikhailov M.A. Legal and ethical aspects of the distribution and use of human identification systems by electronic face recognition, in: Mikhailov M.A. (ed.). *Problemy polucheniya i ispol'zovaniya dokazatel'stvennoi i*

kriminalisticheski znachimoi informatsii, materials of the International Scientific and Practical Conference, Simferopol, Arial Publ., 2019, pp. 79–82. (In Russ.).

16. Williams C.C., Kayaoglu A. The coronavirus pandemic and Europe's undeclared economy: impacts and a policy proposal. *South East European Journal of Economics and Business*, 2020, vol. 15, iss. 1, pp. 80–92. DOI: 10.2478/jeb-2020-0007.

17. Lungu E.V. Pandemic COVID-19. A new challenge to constitutional relations. *Pravoprimenenie = Law Enforcement Review*, 2020, vol. 4, no. 3, pp. 69–75. DOI: 10.24147/2542-1514.2020.4(3).69-75. (In Russ.).

18. Blazheev V.V., Egorov M.A. (eds.). *Legal regulation of artificial intelligence in a pandemic and infodemic*. Moscow, Prospekt Publ., 2020. 240 p. (In Russ.).

19. Egorova M.A., Minbaleev A.V., Kozhevina O.V., Duflo A. The main directions of legal regulation of the use of artificial intelligence in a pandemic. *Vestnik Sankt-Peterburgskogo gosudarstvennogo universiteta. Pravo = Bulletin of St. Petersburg University. Law*, 2021, vol. 12, no. 2. pp. 250–262. DOI: 10.21638/spbu14.2021.201. (In Russ.).

20. Anisimov V.A., Sagitov A.M., Khusnutdinova E.K., Lutsenko V.I., Chemeris A.V., Aminev F.G. Genomic registration of the entire population and ethical issues of the formation and use of relevant databases, in: *Aktual'nye problemy sudebno-ekspertnoi deyatel'nosti v ugolovnom, grazhdanskom, arbitrazhnom protsesse i po delam ob administrativnykh pravonarusheniyakh*, Materials of the VII International Scientific and Practical Conference, November 9, 2018, Ufa, Bashkir State University Publ., 2018, pp. 16–22. (In Russ.).

21. Matveev Yu.N. Technologies for biometric identification of a person by voice and other modalities. *Vestnik Moskovskogo gosudarstvennogo tekhnicheskogo universiteta im. N.E. Baumana = Bulletin of Bauman Moscow State Technical University*, 2012, no. 3 (3), p. 5. DOI: 10.18698/2308-6033-2012-3-91. (In Russ.).

22. Westerlund M. The Emergence of Deepfake Technology: A Review. *Technology innovation management review*, 2019, vol. 9, iss. 11, pp. 39–52.

23. Fitzgerald A. Our Deepfake Future. *Virginia Quarterly Review*, 2020, vol. 96, no. 1, pp. 8–13.

24. Zendran M., Rusiecki A. Swapping Face Images with Generative Neural Networks for Deepfake Technology – Ex-perimental Study. *Procedia computer science*, 2021, vol. 192, pp. 834–843.

25. Qunjian Wu, Ying Zeng, Chi Zhang, Li Tong, Bin Yan. An EEG-Based Person Authentication System with Open-Set Capability Combining Eye Blinking Signals. *Sensors (Basel)*, 2018, vol. 18, iss. 2, art. 335. DOI: 10.3390/s18020335.

26. Hui-Ling Chan, Po-Chih Kuo, Chia-Yi Cheng, Yong-Sheng Chen. Challenges and Future Perspectives on Electroencephalogram-Based Biometrics in Person Recognition. *Frontiers in Neuroinformatics*, 2018, vol. 12, art. 66. DOI: 10.3389/fninf.2018.00066.

27. Ushmaev O.S. Biometric Iris Identification: Current State and Prospects, in: *Grafikon'2011*, 21st International Conference on Computer Graphics and Machine Vision, Moscow, MAKS Press Publ., 2011, pp. 192–194. (In Russ.).

28. Barsukov S.S. Forensic identification by the iris and retina: Modern possibilities and problems of application. *Yurist-Pravoved = Lawyer-Pravoved*, 2021, no. 1 (96), pp. 170–175. (In Russ.).

29. Eremenko Yu.I., Olyunina Yu.S. On the identification of users' keyboard handwriting. *Prospects for the development of information technologies*, 2016, no. 28, pp. 145–151. (In Russ.).

30. Uvarova A.V., Veshchev E.A. Identification by keyboard handwriting, in: *Integratsiya nauki i obrazovaniya*, Collection of articles based on the materials of the international scientific-practical conference, Irkutsk, Apeks publ., 2017, pp. 27–30. (In Russ.).

31. Razumov E.A. Digital dictatorship: features of the social credit system in China. *Trudy instituta istorii, arkheologii i etnografii DVO RAN = Proceedings of the Institute of History, Archeology and Ethnography of the Far Eastern Branch of the Russian Academy of Sciences*, 2019, no. 24, pp. 94–95. (In Russ.).

32. Pinkevich T.V., Nesterenko A.V. Violation of privacy when using big data technology. *Yuridicheskaya nauka i praktika: Vestnik Nizhegorodskoi akademii MVD Rossii = Legal Science and Practice: Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*, 2019, no. 3 (47), pp. 143–147. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Михайлов Михаил Анатольевич – кандидат юридических наук, доцент, доцент кафедры уголовного права и процесса
Севастопольский государственный университет

INFORMATION ABOUT AUTHORS

Mikhail A. Mikhailov – PhD in Law, Associate Professor; Associate Professor, Department of Criminal Law and Procedure
Sevastopol State University

ISSN 2658-4050 (Online)

299011, Россия, г. Севастополь, ул. Университетская, 33
E-mail: mmikh1@ya.ru
SPIN-код РИНЦ: 7307-3426; AuthorID: 189185

Кокодей Татьяна Александровна – доктор экономических наук, доцент, профессор (заведующий) кафедры педагогики и психологии творческого развития
Севастопольский государственный университет
299011, Россия, г. Севастополь, ул. Университетская, 33
E-mail: tanya.kokodey@gmail.com
SPIN-код РИНЦ: 4665-9541; AuthorID: 840438

БИБЛИОГРАФИЧЕСКОЕ ОПИСАНИЕ СТАТЬИ

Михайлов М.А. Цифровые инновации и права человека: дилеммы международной правоохранительной практики / М.А. Михайлов, Т.А. Кокодей // Правоприменение. – 2022. – Т. 6, № 3. – С. 120–133. – DOI: 10.52468/2542-1514.2022.6(2).120-133.

33, Universitetskaya ul., Sevastopol, 299011, Russia
E-mail: mmikh1@ya.ru
RSCI SPIN-code: 7307-3426; AuthorID: 189185

Tatiana A. Kokodey – Doctor of Economics, Associate Professor; Professor (Head), Department of Pedagogy and Psychology of Creative Development
Sevastopol State University
33, Universitetskaya ul., Sevastopol, 299011, Russia
E-mail: tanya.kokodey@gmail.com
RSCI SPIN-code: 4665-9541; AuthorID: 840438

BIBLIOGRAPHIC DESCRIPTION

Mikhailov M.A., Kokodey T.A. Digital innovation and human rights: dilemmas in international law enforcement practice. *Pravoprimenenie = Law Enforcement Review*, 2022, vol. 6, no. 3, pp. 120–133. DOI: 10.52468/2542-1514.2022.6(2).120-133. (In Russ.).