Задача обеспечения тайны идентификации в информационном праве

Наумов В.Б.[*]

Ключевые слова: *цифровая экономика, институт тайн, обезличивание персональных данных, большие данные, законодательство, правоприменительная практика, институт идентификации, принципы идентификации.*

Аннотация. *В статье рассматриваются вопросы развития правоприменения в сфере идентификации в цифровой экономике и закономерности, связанные с идентификацией с использованием больших данных и соотношением институтов тайн и сферы идентификации; предлагается система принципов правового регулирования и обосновывается необходимость введения нового вида тайны — тайны идентификации.*

DOI: 10.21681/2226-0692-2019-3-70-75

В развивающуюся цифровую эпоху увлечение человечества технологиями становится повсеместным. Их удобство и новые горизонты, которые раскрывают большие данные, искусственный интеллект, беспилотный транспорт, аддитивные технологии трехмерной печати и многое другое, могут придать новое качество развития планете. Однако многие технологии могут не только использоваться ради блага и на пользу человеку, но и нести в себе опасности, особенно если человек, общество, бизнес и даже государство не понимают, как они устроены и каковы возможные пределы их надежного и безопасного использования.

Одной из сфер, где оборотная сторона использования технологий может быть обращена против прав и интересов субъектов информационных правоотношений, является сфера удаленной идентификации субъектов посредством разнообразных современных технологий. Все уже привыкли осуществлять удаленные коммуникации, заключать ответственные сделки посредством электронного документооборота, производить банковские транзакции, никогда не появляясь в отделениях банка. Удобство уже созданных технологических решений и, главное, повсеместное распространение дешевых технологий доступа в Интернет и разнообразных мобильных устройств создали все условия для роста популярности удаленной идентификации.

При этом мало кто задумывается, что произошел кардинальный массовый «разрыв» в существовавших тысячелетиями особенностях правоотношений взаимодействия субъектов, когда — ранее и еще до сих пор — индивид, пользуясь своими чувствами и знаниями, способностью анализировать, почти безошибочно узнавал другого, идентифицировал, с кем он общается. Теперь же, потеряв непосредственный контакт с контрагентом, банкиром, знакомым, чиновником, индивид целиком вынужден полагаться на имеющиеся технологии удаленной идентификации субъектов.

Однако эта сфера явно не является столь надежной, как кажется. Неслучайно в существующих в России программных документах развития страны специально выделяются угрозы в сфере идентификации. На проблематику идентификации в сфере регулирования и государственного управления было обращено отдельное внимание в 2017 году при формировании идеологии Программы «Цифровая экономика Российской Федерации»[2], где впервые на государственном уровне был поднят вопрос о том, насколько важна проблематика идентификации для государства: «*Развитию цифровой экономики России сегодня препятствуют новые вызовы и угрозы, прежде всего … проблема обеспечения прав человека в цифровом мире, в том числе при идентификации (соотнесении человека с его цифровым образом), сохранности цифровых данных пользователя, а также проблема обеспечения доверия граждан к цифровой среде…*».

Сообразно названной угрозе была обозначена и задача (п.1.1 Программы) создания правовых условий

[2] Программа «Цифровая экономика Российской Федерации», утв. Распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р. [Электронный ресурс]. СПС «КонсультантПлюс» (дата обращения: 06.08.2019). Прим.: документ утратил силу с 12 февраля 2019 года в связи с изданием распоряжения Правительства РФ от 12.02.2019 № 195-р.

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16013 «Исследование концептуальных подходов к формированию системы правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе».

[*] ***Наумов Виктор Борисович***, кандидат юридических наук, доцент, старший научный сотрудник сектора информационного права и международной информационной безопасности Института государства и права РАН, г. Москва, Российская Федерация.

E-mail: nau@russianlaw.net

для формирования единой цифровой среды доверия, которая обеспечит участников цифровой экономики средствами «*доверенных цифровых дистанционных коммуникаций*» для того, чтобы обеспечить, в частности, удаленное подтверждение личности для совершения юридически значимых действий и различных способов идентификации и аутентификации лиц.

Чуть позже в паспорте проекта Национальная программа «Цифровая экономика Российской Федерации»[3] в разделе 4.1 Федерального проекта «Нормативное регулирование цифровой среды» появилось дополнение, касающееся сферы идентификации и указывающее на необходимость регулирования особого порядка использования персональных данных, которые повсеместно собираются и используются для идентификации физических лиц, а именно — должны быть обеспечены «*благоприятные правовые условия для сбора, хранения и обработки данных с использованием новых технологий, в части установления порядка обезличивания персональных данных, условий и порядка их использования, уточнения ответственности за их ненадлежащую обработку, порядка получения согласия на их обработку*» (п. 1.3. указанного раздела).

Важно отметить, что идентификация должна быть присуща не только экономическим отношениях и стимулировать исключительно коммерческие цели ее развития, но и быть связана с гуманитарными и культурными задачами, в числе которых, как справедливо отмечают Т.А. Полякова и А.В. Минбалеев, и стратегическая задача формирования «*электронного пространства знаний*», где связь объектов и субъектов и информационная безопасность последних играют значимую роль [6, с. 236].

Проблемы неправильной идентификации постепенно становятся повсеместными и уже приводят к негативным последствиям. Ряд исследователей при этом считает, что, в частности, «*массовое использование систем биометрической идентификации характерно для стран с высоким уровнем правонарушений в сфере документооборота и неустойчивыми традициями защиты частной жизни (примеры: Индия, Буркина-Фасо, Колумбия и др.)*» [7, с. 42]. Но не только указанные страны столкнулись с комплексными проблемами в рассматриваемой сфере. Так, характерный случай мошенничества произошел недавно в Великобритании. Жертвой стал гендиректор британской энергетической компании, который, разговаривая по телефону с вышестоящим начальником, получил от него указание перечислить большую сумму денег контрагенту, что и было сделано. Понял он, что происходит неладное, только после второго запроса «начальника» на организацию нового перевода[4].

Совсем недавно по лентам российских информагентств прошла новость о том, к чему привела несовершенная организация идентификации. По данным Интернет-издания «Фонтанка.Ру», в августе 2019 года в Санкт-Петербурге произошло очередное дорожно-транспортное происшествие. Один из его участников, управлявший каршеринговым автомобилем, предположительно, являлся несовершеннолетним и управлял автомобилем без водительского удостоверения. По информации издания, аккаунт для пользования автомобилями службы каршеринга он купил примерно за 3500 рублей[5]. В результате его действий был причинен ущерб другим участникам движения и пешеходу. Очевидно, что созданная в этом случае организационно-правовая и техническая система идентификации дала сбой.

Нужно признать, что на современном этапе развития технологий уже многое может быть сгенерировано в обход разработанных технологий удаленной идентификации. Эти решения или «решения» становятся все дешевле, что позволяет делать это уже несведущим в нюансах алгоритмов обработки изображений людям. Возник специальный термин «DeepFake»[6] и существует свободно распространяемое программное обеспечение, например, заменяющее изображения лица человека в существующем видео, также разработаны программы, которые с помощью специальных алгоритмов выявления характерных поз и движений и их генерации, создают видеоряд несуществующих действий, который выглядит так, как будто бы эти движения и действия совершал реальный человек.

При всей популярности сейчас идей широкого распространения видеонаблюдения и фиксации, биометрической идентификации по изображениям, в том числе при внедрении норм о них в законодательство, настоящим ударом для них станут подделки видеоизображений в реальном режиме времени, когда ни системы, ни люди не смогут без специального аппаратно-программного обеспечения различать, что является подлинным, что — сгенерированным и, чаще всего, с незаконными или недобросовестным целями.

Но даже без недобросовестной генерации или подмены видеоинформации в мире стали обращать внимание на то, что удобные и развивающиеся технологии могут способствовать нарушению прав и интересов граждан. Здесь показателен пример США, где в Сенат был внесен законопроект о конфиденциальности коммерческого распознавания лиц[7]. Согласно законопроекту, запрещено использовать технологию распознавания лиц без явного согласия физического лица на ее использование в его отношении. При этом из сферы действия закона исключены правоотношения в сфере государственного управления и безопасности.

В мае этого года издания о технологиях распространили новость, что Окружной совет Сан-Франциско запретил использование биометрической идентифика-

---

[3] Утвержден протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7. [Электронный ресурс]. СПС «КонсультантПлюс» (дата обращения: 05.08.2019).

[4] Голос как у начальника — не отличишь: как искусственный интеллект позвонил и украл сотни тысяч долларов [Электронный ресурс]. URL: https://www.bfm.ru/news/423702 (дата обращения: 06.09.2019).

[5] Водителю на каршеринге, устроившему массовое ДТП на Лиговском, оказалось 16 лет. Аккаунт он купил [Электронный ресурс]. URL: https://m.fontanka.ru/2019/08/15/019/ (дата обращения: 06.08.2019).

[6] Условно его можно перевести как «качественная подделка».

[7] The Commercial Facial Recognition Privacy Act [Электронный ресурс] // Congress. 2019. Режим доступа: https://www.congress.gov/bill/116th-congress/senate-bill/847 (дата обращения: 6.09.2019).

ции для использования полицией и иными контрольно-надзорными органами. Решение было принято 8 голосами к 1, и это делает Сан-Франциско первым крупным американским городом, заблокировавшим инструмент, к которому обращаются многие полицейские в поисках как мелких подозреваемых в совершении преступлений, так и подозреваемых в террористических актах.

Распоряжение Окружного совета Сан-Франциско[8] о внесении изменений в Административный Кодекс штата направлено на ограничение не только технологии распознавания лиц, но и всех «технологий наблюдения»[9]. Распоряжение также ограничит местную полицию в передаче информации федеральным агентствам (например, по иммиграционному и таможенному контролю). При этом ограничения не будут применяться в международном аэропорту Сан-Франциско, где действует юрисдикция федеральных агентств — они могут свободно использовать системы распознавания лиц и биометрические сканеры по своему усмотрению.

В это же время в штате Иллинойс был принят Закон о видеоинтервью с использованием искусственного интеллекта[10]. Закон предусматривает, что работодатель, который просит соискателей записать видеоинтервью с их участием и использует аналитические данные, полученные из предоставленных соискателями видеофайлов с помощью методов искусственного интеллекта, должен перед собеседованием уведомить каждого соискателя в письменном виде о том, что программа, содержащая методы искусственного интеллекта, может использоваться для анализа выражений лица соискателя и для рассмотрения пригодности соискателя на должность, перед собеседованием объяснить, как работает программа, и какие характеристики она использует для оценки соискателей, а затем получить письменное согласие соискателя на оценку его записанного на видео поведения программой. Закон штата Иллинойс запрещает работодателю передавать третьим лицам видеоизображение соискателя, за исключением лиц, чей опыт или технологии необходимы для оценки пригодности соискателя на должность, а после обработки информации для целей трудоустройства в течение 30 дней она должна быть удалена.

В России такие социально-технологические проблемы пока недостаточно урегулированы на законодательном уровне. Предметное регулирование начало формироваться с 1995 года, когда было введено понятие персональных данных, содержание которых было определено через задачу идентификации физических лиц. После этого в различных отраслях законодательства, в первую очередь информационном, стали появляться узкоспециальные нормы, касающиеся тех или иных процессов идентификации. Развивается регулирование в системе государственных услуг [5], финансового законодательства, определяющего упрощенную и обычную идентификацию [4], нотариата, связи, телемедицине, законодательстве об электронной подписи и электронном документообороте, других отраслях [подр. см. 3], принята также новая редакция пункта 1 статьи 160 Гражданского кодекса (вступает в силу с 1 октября 2019 года) о соблюдении письменной формы сделки, ссылающаяся на способ, позволяющий достоверно определить лицо, выразившее свою волю в рамках нее.

Два важных события для развития предметного законодательства об идентификации имели место в 2013 и 2018 годах, когда информационное законодательство было дополнено нормами о новых Единой системе идентификации и аутентификации[11] и Единой биометрической системе[12].

В сфере идентификации в России имеется обширная судебная практика — потребность в идентификации субъектов в информационном пространстве становится очевидной в самых различных категориях дел. Например, в Постановлении Арбитражного суда Уральского округа от 4 марта 2019 года по делу № А50-13021/2017 указывалось, что «*заявитель в кассационной жалобе приводит довод о том, что <…> представленная в материалы дела анонимная переписка двух лиц «(ФИО убрано)» (av.zaharov_perm@mail.ru) и «gsv20175@mail.ru» не может быть принята в качестве доказательства в силу своей анонимности, в связи с тем, что не позволяет идентифицировать лиц, ведущих переписку, тем более их полномочия.*» Несмотря на это, кассационный суд решил, что нижестоящими судами правильно «*учтена переписка между сторонами, из которой усматривает-*

[8] Administrative Code — Acquisition of Surveillance Technology [Электронный ресурс] // The Committee on Information Technology. 2019. URL: https://sfgov.legistar.com/View.ashx?M=F&ID=7206781&GUID=38D37061-4D87-4A94-9AB3-CB113656159A (дата обращения: 6.09.2019).

[9] В решении Окружного совета Сан-Франциско под «технологиями наблюдения» (англ. "surveillance technology") понимается весьма широкий круг объектов — симуляторы сотовой связи, автоматические считыватели номерных знаков, оборудование и услуги для обнаружения огнестрельного оружия, видео- и аудио-технологии мониторинга и / или записи и т. п.

[10] The Artificial Intelligence Video Interview Act [Электронный ресурс] // General Assembly. 2019. URL: https://legiscan.com/IL/bill/HB2557/2019 (дата обращения: 6.09.2019).

[11] О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и Федеральный закон «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» [Электронный ресурс]: Федеральный закон от 7 июня 2013 г. № 112-ФЗ. СПС «КонсультантПлюс» (дата обращения: 6.09.2019). Совместно с Правилами использования федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» [Электронный ресурс]: утв. Постановлением Правительства РФ от 10 июля 2013 г. № 584 (в ред. Постановлений Правительства РФ от 28. окт. 2013 № 968, от 30.06.2018 № 772). СПС «КонсультантПлюс» (дата обращения: 6.09.2019).

[12] Федеральный закон от 31 декабря 2017 года № 482-ФЗ О внесении изменений в отдельные акты Российской Федерации. Совместно с «Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных в целях идентификации, порядка размещения и обновления биометрических персональных данных в единой биометрической системе, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации» (Зарегистрировано в Минюсте России 04.07.2018 № 51532) [Электронный ресурс]: Приказ Минкомсвязи России от 25 июня 2018 г. № 321. СПС «КонсультантПлюс» (дата обращения: 6.09.2019).

ся, что истец признавал факт согласования условий по оплате именно по цене 1 500 000 руб.»[13].

Тот же суд в другом споре сделал прогрессивный вывод о том, что «*сформировался деловой обычай общения путем обмена электронными письмами на электронные адреса (e-mail), позволявшие им идентифицировать каждого из адресата, в том числе по содержимому отправлений*»[14].

Процессуальное значение может иметь еще одно обстоятельство, на которое еще два года назад, обобщив практику, указал Президиум Суда по интеллектуальным правам: «*затруднительность идентификации отправителя и адресата может не позволять считать такую переписку относимой к рассматриваемому спору, поскольку отсутствует возможность корреляции такой информации со спорящими сторонами и отношениями между ними. Если же обе «переписывающиеся» стороны подтвердят факт ее существования, такое доказательство может быть признано относимым при отсутствии иных препятствий*»[15].

Парадоксально, но факт — резко возросшее по объему и количеству норм регулирование в сфере идентификации, значительная судебная практика и административная практика органов исполнительной власти[16] до сих пор не опираются на единую терминологическую базу, не имеют системы принципов и развиваются таким образом, что нормы из различных отраслей права и законодательства активно конкурируют друг с другом, регулируя при этом сходные по своим задачам идентификации субъектов и содержанию взаимодействия правоотношений[17]. Только сейчас в системе инициатив «Цифровой экономики Российской Федерации»[18]начато широкое обсуждение нескольких подготовленных законопроектов о внесении изменений в отдельные законодательные акты Российской Федерации в части совершенствования процедур идентификации и упрощенной идентификации, где акцент делается на изменениях в законодательстве о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, законодательстве о национальной платежной системе, в совокупности с информационным законодательством, при этом также предлагаются изменения для внесения в законодательство о персональных данных.

Последнее происходит с целью обеспечения расширения пределов использования указанных данных за счет производимого их обезличивания. Этот механизм важен для ситуаций, когда не требуется производить или запрещено производить идентификацию граждан, но содержащаяся в электронных сообщениях, записях баз данных, информационных ресурсах иная информация представляет ценность, в первую очередь, для всевозможных сервисов в сфере цифровой экономики.

В 2018 году юридическая фирма Dentons выполнила комплексное исследование «Определение состава сведений, составляющих соответственно банковскую тайну, тайну связи, врачебную тайну и иные виды тайн, и порядка их передачи третьим лицам»[19], проведенное по заказу Центра компетенции по нормативному регулированию Цифровой экономики — «Фонд Сколково» в соответствии с пунктом 01.01.003.003 Плана мероприятий по направлению «Нормативное регулирование» программы «Цифровая экономика Российской Федерации».

Ключевым идеологическим лейтмотивом исследования послужила задача обеспечения возможности использования конфиденциальной информации в системе различных видов тайн (банковская тайна, налоговая тайна, тайна связи, врачебная тайна, коммерческая тайна и иные виды тайн) для оказания услуг, развиваемых в цифровую эпоху. Решение этой задачи не является простым, поскольку, с одной стороны, институты тайн и конфиденциальной информации объективно препятствуют свободному, в том числе, коммерческому использованию тех или иных сведений, включая персо-

[13] Постановление Арбитражного суда Уральского округа от 04 марта 2019 года по делу № А50-13021/2017 [Электронный ресурс]. // URL: http://kad.arbitr.ru/Document/Pdf/39720007-262d-4a0b-8ddc-3e9ebc12dfa8/130a7afd-416d-4a87-a4b7-51bb48ea96a7/A50-13021-2017_20190304_Reshenija_i_postanovlenija.pdf (дата обращения: 6.09.2019).

[14] Постановление Арбитражного Суда Уральского Округа от 13 февраля 2018 г. по делу № А60-23408/2015 [Электронный ресурс]. СПС «КонсультантПлюс» (дата обращения: 06.08.2019).

[15] Информационная справка, подготовленная по результатам обобщения судебной практики Суда по интеллектуальным правам в качестве суда первой и кассационной инстанций с учетом практики Верховного Суда Российской Федерации по некоторым вопросам, возникающим при оценке доказательств, содержащих информацию, размещенную в сети Интернет [Электронный ресурс]: Постановление президиума Суда по интеллектуальным правам от 14 сентября 2017 г. № СП-23/24. СПС «КонсультантПлюс» (дата обращения: 6.09.2019). Постановление Суда по интеллектуальным правам от 3 октября 2016 г. по делу № А40-138017/2013 [Электронный ресурс]. СПС «КонсультантПлюс» (дата обращения: 04.08.2019).

[16] За последние годы проблематика идентификации чаще всего стала встречаться в Российской Федерации в практике Федеральной антимонопольной службы. В подавляющем большинстве случаев это связано с делами о законности рекламных рассылок, столь массово эти десятилетия преследующих граждан по смс и электронной почте. Здесь, поскольку бремя доказывания получения наличия согласия на получение рассылки согласно ст. 18 Федеральный закон «О рекламе» лежит на рекламораспространителе, именно последние должны в административном разбирательстве доказывать, как они идентифицировали абонента или пользователя и получили от него указанное согласие. Органы ФАС РФ строят свою логику на названной выше норме и п. 15 Постановления Пленума ВАС РФ от 08.10.2012 № 58 «О некоторых вопросах практики применения арбитражными судами Федерального закона «О рекламе», где указано, что ФЗ «О рекламе» «*не определяет порядок и форму получения предварительного согласия абонента на получение рекламы по сетям электросвязи, то, следовательно, согласие абонента может быть выражено в любой форме, достаточной для его идентификации и подтверждения волеизъявления на получение рекламы от конкретного рекламораспространителя*».

[17] Подробнее см.: Наумов В.Б. Негативные закономерности формирования понятийного аппарата в сфере регулирования Интернета и идентификации // Информационное право. 2018. № 1. С. 32—39.

[18] Об утверждении программы «Цифровая экономика Российской Федерации» (утр. силу) [Электронный ресурс]: с. 74 Распоряжения Правительства РФ от 28 июля 2017 г. № 1632-р. СПС «КонсультантПлюс» (дата обращения: 06.08.2019).

[19] 01.01.003.003.002. Исследование по определению состава тайн_Итог / [сайт Сколково, URL: https://sk.ru/foundation/legal/m/sklegal03/22588/download.aspx (дата обращения: 08.08.2019). Руководители и соавторы НИР: В.Б. Наумов, В.В. Архипов; исполнители НИР, соавторы: Р.А. Ахобекова, Т.А. Бовсуновская, Я.В. Бутримович, А.В. Грачева, Е.М. Крамм, С.П. Лялькова, В.О. Полыгалов, К.М. Смирнова, Е.В. Тытюк. Объектом исследования выступили законодательство и правоприменительная практика в России, ЕС и входящие в него страны, Великобритании, США, Японии, Сингапуре, Южной Корее, Израиле, ОАЭ и ряде других стран.

нальные данные, с другой, собираемая банками, операторами связи, Интернет-бизнесом, страховыми и транспортными компаниями, медицинскими учреждениями информация может быть использована как для улучшения качества соответствующих услуг, так и для развития цифровой экономики.

Сравнивая юрисдикции, был выявлен ряд важных закономерностей, свойственный подавляющему большинству государств. Среди них — отсутствие исчерпывающего сбалансированного перечня видов данных, составляющих тайны, и свойственная законам всех стран ситуация, когда одни и те же данные могут составлять различные виды регулируемой информации. Последнее очевидно на примере персональных данных, которые могут одновременно включаться в состав различных тайн — от медицинской до тайны связи.

Существенным представляется факт, что многие страны мира сейчас сосредоточились на разработке правовых решений обеспечения оборота больших данных, где ключевой идеей возможности введениях их в оборот как раз и является использование процедур обезличивания информации таким образом, чтобы дальнейшая идентификация субъектов была невозможна. Так, KoreaTelecom предлагала доступ к анонимизированным данным, содержащим данные о текстах пользовательских сообщений и мест звонков с целью поддержки транспортного планирования — оптимизации работы ночного транспорта и решения проблем с перегруженным трафиком; эстонские операторы связи вправе обрабатывать данные о месте нахождения пользователей при условии предварительной анонимизации[20]. Кроме того, анонимизация или де-идентификация персональных данных в США занимает большое место в разрешении проблем, возникающих в связи с технологией больших данных. Используются для этих целей самые разнообразные методы - маскирование данных, добавление шумов, скремблирование букв, кодирование и т. д.[21]. В этой связи интересен также опыт Японии. Согласно Отчету об использовании анонимной информации, подготовленному японским ведомством в сфере защиты персональной информации[22], адреса электронной почты, номера телефонов отнесены к информации, которая может идентифицировать персональную информацию. В Японии существует концепция т. н. «связующих кодов» («codeslinking»), именно они используются для организации алгоритмов анонимизации. Отчет предусматривает, что для создания обезличенной информации связующие коды, которые могут быть использованы для идентификации лица, должны быть удалены[23].

Важно отметить (это важно и для идентификации), что в мире пока не существует четкого технического и, соответственного, юридического ответа в отношении следующего важного аспекта работы с большими данными. Можно предположить, что при обработке и (обычно) непрерывном процессе сбора больших данных, откуда будут удалены все персональные данные, будут, тем не менее, возникать ситуации, когда снова будет появляться возможность повторной идентификации физических лиц. Чтобы соответствующие риски были минимизированы, потребуется введение в законодательство четкого разграничения «обратимого» и «необратимого» обезличивания информации.

Таким образом, регулирование идентификации должно происходить в неразрывной связи с задачей обезличивания с учетом растущей популярности больших данных, для чего для развития регулирования потребуется сбалансированный единый набор идей.

В целом можно заключить, что в сфере идентификации возрастают интересы и объективная роль государства, и уже имеющаяся совокупность норм, построенная вокруг однородных правоотношений, позволяет говорить о самостоятельном правовом институте идентификации субъектов, значение которого будет только возрастать. Согласно определению И.Л. Бачило, «*институтами информационного права являются такие блоки правовых актов и норм, которые, будучи сгруппированы по единой цели, обеспечивают регулирование отношений, связанных с формированием и использованием информационных ресурсов, информационных и коммуникационный технологий, очерчивают цели инновационных процессов на основе ИКТ, мобилизуют законодателя и правоприменителей на удовлетворение потребностей субъектов права в информационной сфере*» [1, с. 128]. Все перечисленные классиком информационного права признаки можно наблюдать и в сфере правового регулирования идентификации.

В этих обстоятельствах информационному праву отводится ключевая роль: оно должно предложить терминологический аппарат для идентификации и сбалансированную систему принципов правового регулирования.

Последняя должна учитывать потребности не только информационного, но и других отраслей права и быть, по возможности, единой для всей системы права. В их основе должны быть, как пишет П.У. Кузнецов о праве в целом и об информационном праве в частности, идеи права и они должны определять *руководящие положения* рассматриваемой задачи [2, с. 58]. Для этого в рассматриваемой задаче нужно ограничиться наиболее важными конструкциями, в числе которых возможно предложить для дальнейшего научного обсуждения три принципа — добровольность, соразмерность и конфиденциальность идентификации.

---

[20] 01.01.003.003.002. Исследование по определению состава тайн_Итог / [сайт Сколково, URL: https://sk.ru/foundation/legal/m/sklegal03/22588/download.aspx, с. 337 (дата обращения: 06.08.2019).

[21] Dr. Khaled El Elmam, Health Data De-Identification [Электронный ресурс] // The International Association of Privacy Professionals (IAPP) [Site]. URL: https://iapp.org/media/pdf/knowledge_center/Perspectives_ on_Health_Data_De-Identification_final.pdf (дата обращения: 27.07.2018).

[22] The PPC Secretariat Report on Anonymously Processed Information [Электронный ресурс]: Personal Information Protection Commission of Japan // Personal Information Protection Commission of Japan. URL: https://www.ppc.go.jp/en/legal/ (дата обращения: 08.08.2018).

[23] 01.01.003.003.002. Исследование по определению состава тайн_Итог / [сайт Сколково, URL: https://sk.ru/foundation/legal/m/sklegal03/22588/download.aspx, с. 290 (дата обращения: 06.08.2019).

Для разработки содержания указанных принципов важно, чтобы идентификация привела к искомому результату — достоверному установлению конкретного лица, участвующего в отношениях, либо установлению иных требуемых обстоятельств, связанных с действиями лица, участвующего в идентификации. Это задача должна быть ключевой для разработки правовой модели регулирования и формирования института идентификации и системного законодательства.

Первый указанный принцип основан на идее, что если нет специального требования в законе, например, в связи с обеспечением интересов в сфере государственной безопасности, то лицо должно иметь право выбора, участвовать ли в процессе идентификации или нет. Этот принцип также должен быть связан с уведомлением лиц о наличии процессов идентификации с обеспечением возможности в них не участвовать.

Второй принцип также связан с прозрачностью целей и задач реализации предметных правоотношений и должен определять требование к идентифицирующему лицу осуществлять идентификацию только в тех пределах, в которых требуются использовать результаты идентификации. Скажем, когда идентификация требуется только для того, чтобы установить, взаимодействует ли программа-бот или человек[24], не должно происходить идентификации конкретного пользователя. Принцип соразмерности также должен определять качество и надежность используемых организационно-технических и правовых механизмов, определяющих условия процессов идентификации.

Третий принцип представляется самым сложным по своему содержанию. Конфиденциальность идентификации можно рассматривать через новую специальную категорию — тайну идентификации.

Очевидно, что для идентифицируемого не должны быть нарушены его права и интересы путем разглашения как используемой для идентификации информации, так и ее результатов.

Также важно, чтобы не пострадали права и интересы идентифицирующего, а именно, чтобы не стали известны используемые алгоритмы и решения идентификации. Если они будут раскрыты, то идентификация может быть недостоверной, когда с умыслом или без него ее будут обходить, как это было описано в примерах в начале статьи. В этой связи лицо, организующее идентификацию либо оказывающее услуги проведения идентификации, должно иметь право сохранять в тайне технологии идентификации и этот статус должен быть установлен законом по умолчанию.

И, наконец, третий элемент предлагаемой тайны, определяющей содержание соответствующего принципа — это сохранение в тайне самого факта идентификации, если иное не следует из обстоятельств и требований организации процесса идентификации, договора или закона. В этом, в общем случае, могут быть заинтересованы все субъекты правоотношений.

Завершая настоящую работу, необходимо отметить, что без гармонизации системы определений, установления единого состава объектов и субъектов в сфере идентификации и определения ее правовых принципов разработка нового специального законодательства в сфере удаленной идентификации невозможна. Решение задач обеспечения надежности и безопасности идентификации в широком ее смысле также должно сопровождаться введением ответственности за неправильную или неполную идентификацию в том случае, если ее неверный результат привел к каким-либо негативным последствиям. Появление полноценного законодательства в этой сфере позволит говорить об успешном становлении такого института права, как институт идентификации. При этом важно иметь в виду, что если удастся в ближайшем будущем создать систему правового регулирования доверенных коммуникаций, то будет сделан важный шаг в обеспечении безопасности идентификации субъектов правоотношений в цифровую эпоху.

Литература

1. Бачило И. Л. Информационное право: учебник для академического бакалавриата / И. Л. Бачило. 5-е изд., перераб. и доп. М. : Издательство Юрайт, 2019. 419 с.
2. Информационное право: учебник / Кузнецов П.У. М. : Юстиция, 2017. 336 с. С. 58.
3. Наумов В.Б. Научные подходы к классификации видов правовой идентификации в информационных правоотношениях // Труды Института государства и права Российской академии наук. 2016. № 3. С. 104—115.
4. Наумов В.Б., Брагинец А.Ю. Информационно-правовые проблемы удаленной идентификации субъектов в сфере финансовых услуг // Информационное право. 2016. № 1. С. 13—19.
5. Наумов В.Б., Полякова Т.А. Правовые проблемы идентификации субъектов в государственных и негосударственных системах в России // Вестник Академии права и управления. 2016. № 2 (43). С. 14—21.
6. Полякова Т.А., Минбалеев А.В. Формирование единого российского электронного пространства знаний как стратегическая задача обеспечения информационной безопасности в Российской Федерации / Сборник трудов конференции «Информационные технологии и право: правовая информатизация» — 2018, Минск, 17 мая 2018 г.
7. Ярков В.В., Ренц И.Г. Действительность принципов нотариата в XXI веке: новые вызовы // Закон. 2019. № 7.

Рецензент: Полякова Татьяна Анатольевна, *доктор юридических наук, профессор, заведующий сектором ИГП РАН, г. Москва, Россия. E-mail: inform@igpzan.ru*

[24] Для этого часто используется т. н. «Ка́пча», происходящее от CAPTCHA (англ. Completely Automated Public Turing test to tell Computers and Humans Apart) — «полностью автоматизированный публичный тест Алана Тьюринга для различения компьютеров и людей», придуманный им еще в 1950 году.