УДК 340

В. Б. Наумов

Организационно-правовой анализ развития коммерческих цифровых систем идентификации

В условиях развития информационного общества и распространения новых цифровых технологий одной из ключевых задач является обеспечение прав человека в цифровом пространстве. В нем, как и для цифровой экономики, проблематика идентификации субъектов и объектов, в числе которых выступают информационные системы, компьютерные и цифровые устройства и их программное обеспечение, является одной из ключевых основ создания системы стабильного правоприменения. При этом в сфере правового регулирования идентификации, которая является межотраслевой с позиций права, происходят обширные, но несистемные изменения, которые до сих пор не привели к созданию единого комплекса норм, определяющих предметную терминологию, принципы регулирования и правовой режим идентификации. Для преодоления этой негативной тенденции необходим анализ организационно-правовых основ и массовой практики использования современных цифровых систем идентификации.

In the context of the development of the information society and the spread of new digital technologies, one of the key tasks is to ensure human rights in the digital space. In it, as for the digital economy, the problem of identifying entities and objects, including information systems, computer and digital devices and their software, is one of the key foundations for creating a system of stable law enforcement. At the same time, in the field of legal regulation of identification, which is cross-sectoral from the standpoint of law, extensive but non-systemic changes are taking place that have not yet led to the creation of a single set of norms defining subject terminology, regulatory principles and the legal regime of identification. To overcome this negative trend, an analysis of the organizational and legal foundations and mass practice of using modern digital identification systems is necessary.

Ключевые слова: институт идентификация, информационные процессы, аутентификация, Интернет, информационное общество, идентификаторы, инфраструктура идентификации, биометрия, ответственность и контроль в сфере идентификации.

Key words: Institute identification, information processes, authentication, Internet, information society, identifiers, identification infrastructure, biometrics, responsibility and control in the field of identification.

Идентификация субъектов и объектов давно известна гражданам. Так, гражданин сталкивается с проверкой документов, потребностью «представляться» и анализировать документы других граждан регулярно. В уходящей «эпохе бумажных документов» эти действия не требовали создания специальной системы правового регулирования, достаточно было исполнять подзаконные акты, описывающие, например, порядок установления личности, правила оказания тех или иных услуг. В предшествующие века – в позднем Средневековье, обходились и без документов, приводя свидетелей, как, например, это делали банкиры Тосканы, когда выдавали кредиты или обналичивали векселя. В праве XX в. разные отрасли по-своему решали узкие задачи по идентификации не только субъектов, но и объектов. Многие из отраслей разработали свои специальные подходы к идентификации, скажем, как это произошло в криминалистике и уголовном процессе.

Все поменялось в «эпоху Интернета», когда электронный документооборот стал основой и для большинства видов правоотношений, и для очень многих отраслей права. При этом в последнее десятилетие крупномасштабные процессы цифровой трансформации и распространение технологий Интернета вещей создали организационные и технические возможности для сбора большого количества данных как при использовании технологий людьми, так и благодаря устройствам системы Интернет вещей. Уже сейчас в сфере обработки больших массивов информации развитие технологий искусственного интеллекта создает принципиально новые возможности для идентификации субъектов в сфере распознавания голоса и изображений человека. Нормативно-правовой статус генерируемых огромным количеством информационных систем и устройств больших данных (big data) может стать одним из краеугольных камней бизнеса и государственного управления, при этом его связь с формами тайны и требованиями о неразглашении в самых разных типах правовых отношений еще не определена. Именно большие данные в перспективе могут «перевернуть мир», когда за счет методов их обработки без непосредственного участия в специальных правоотношениях по идентификации субъектов и, что представляется крайне опасным, без информирования последних будет осуществляться установление личности в цифровом мире.

В последнее десятилетие отношение государства к задачам идентификации менялось, и в настоящий момент превалируют идеи введения обязательной идентификации в большинстве сфер жизнедеятельности, а в отечественной науке и практике началась дискуссия о злоупотреблениях механизмами защиты конфиденциальности и усилении общего государственного контроля. Результатом этого стали предложения о введении требований об обязательной идентификации, в ряде случаев – запрете анонимного взаимодействия.

В этих условиях закономерным оказалось принятие Федерального закона от 31.12.2017 № 482-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации», который значительно расширил предметные полномочия органов исполнительной власти, а также ввел в Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» новую ст. 14.1 «Применение информационных технологий в целях идентификации граждан Российской Федерации», закрепив новый вектор развития государственной политики в информационном пространстве – создание единой биометрической системы. Последняя[1] – это цифровая платформа для удаленной биометрической идентификации, которая позволяет предоставлять новые цифровые коммерческие и государственные услуги для граждан в любое время и в любом месте. Система создана по инициативе Центрального банка Российской Федерации и Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. «Ростелеком» – разработчик и оператор Единой биометрической системы. Также на фоне развития регулирования и правоприменения в сфере биометрии началось обсуждение возможностей и тестирование новой методологии создания «цифрового профиля» гражданина [1].

В этих условиях и в связи с наличием обширного правового регулирования автор придерживается позиции, что в России уже сформировался самостоятельный правовой институт идентификации, который востребован на практике[2].

---

[1] См.: Единая биометрическая система. [Электронный ресурс]. URL: https://bio.rt.ru/ (дата обращения: 28.02.2020).

[2] См. подробнее: Наумов В.Б. Научные подходы к классификации видов правовой идентификации в информационных правоотношениях // Труды Института государства и права РАН. 2016. № 3. С. 104-115; Naumov V.B. Information security in identification in the digital age: information law aspect // Государство и право. 2019. № 9. С. 117–130.

Именно практика, где цели и задачи бизнеса в цифровой среде определяют потребности в технологиях идентификации, свидетельствует о *высокой технологической зависимости* предметного правового регулирования от характера и функционирования цифровых технологий.

При этом идентификация представляет собой *информационный процесс*, в котором в зависимости от целей идентификации, содержания и возможностей используемых цифровых технологий реализуются различные этапы и подпроцессы, в числе которых нужно упомянуть регистрацию, аутентификацию, авторизацию и верификацию пользователей. Этапы и подпроцессы в процессе идентификации могут отличаться в зависимости от вида последней[3].

Ключевую роль в процессе идентификации в цифровом пространстве играют идентификаторы, правовое определение которых нуждается в закреплении в законодательстве. Идентификатором, при этом, *должна признаваться любая уникальная информация, связывающая субъект или объект с информацией о нем в информационной системе*. Дискуссионным представляется вопрос о взаимно однозначном соответствии идентификатор – субъект (или объект), поскольку, например, возможна групповая идентификация, где не требуется установление конкретного лица в информационном правоотношении, а только определение, к какой группе он относится (например, является ли он совершеннолетним и т.п.).

Важное значение для бизнеса и государства имеет создание информационных систем идентификации или, как их можно определить, *инфраструктуры идентификации*. В настоящее время во всем мире наблюдается рост количества универсальных технологических решений по идентификации субъектов, как создаваемых государствами, так и распространяемых коммерческими организациями.

Так, в России семь лет назад появилась известная гражданам Единая система идентификации и аутентификаци (далее – ЕСИА)[4]. Очевидно, что в случае государственных инициатив имеет место централизованное управление в сфере идентификации и отсутствует альтернатива выбора провайдеров услуг. В качестве надлежащей идентификации для создания стандартной

---

[3] См. подробнее о взаимосвязи соответствующих понятий и подпроцессов в сфере идентификации в статье Наумова В.Б. Взаимодействие технологий и права в сфере идентификации // Вестник Московского университета. Серия 26: Государственный аудит. 2019. № 2. С.105.

[4] О правовом регулировании ее использования см.: 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.

учетной записи ЕСИА предполагает заполненный профиль пользователя с указанием СНИЛС и данных документа, удостоверяющего личность (паспорт гражданина РФ, для иностранных граждан – документ иностранного государства). Данные проходят проверку в ФМС РФ и Пенсионном фонде РФ. На электронный адрес субъекта идентификации будет направлено уведомление о результатах проверки. Обязанность пользователя предоставить корректные персональные данные и в дальнейшем вводить правильный логин и пароль [4].

Иная логика наблюдается в коммерческой сфере, где централизация не воспринимается в качестве панацеи. Так, в 2006 г. была создана система OpenID, стандарты который обеспечивают возможность использования единой учетной записи для многих информационных систем и сервисов.

Система стала популярной во всем мире, что обусловлено ее удобством для пользователей. При этом, в отличие от многих систем идентификации, включая государственные, OpenID – децентрализованная система и в ней всегда существует возможность выбора провайдера OpenID. Управляет развитием соответствующих стандартов и координирует заинтересованных в методологии лиц OpenID Foundation [8]. Идентификация с использованием Open ID представляет собой вход в сервис через переадресацию на ресурс, где уже была пройдена идентификация. Open ID является наиболее популярным способом в настоящее время[5]. При этом, несмотря на заверения сторонников, он объективно менее надежен, чем государственные инфраструктуры идентификации, и изначально предполагает полное доверие к информации, например в аккаунте социальной сети, где часто удостоверение личности требуется обычно лишь после блокировки аккаунта и сопряжено с дополнительными требованиями к предоставлению документов. Отметим, что при децентрализованных подходах по организации инфраструктуры идентификации высока роль саморегулирования и технического регулирования.

Многообразие технических решений в сфере идентификации возможно наглядно продемонстрировать на примере популярных у граждан интернет- и банковских сервисов. Изначально в них использовались простые организационно-технические решения, где ввода логина и пароля пользователя оказывалось достаточно, по мнению владельца информационной системы идентификации, для идентификации лица. Одним из таких примеров может служить пин-код в процессе использования банковской карты или

[5] См.: OpenID Connect. [Электронный ресурс]. URL: https://openid.net/connect/faq/ (дата обращения: 28.02.2020).

устройства при любых операциях с терминалом или с устройством. К таким примерам также можно отнести и одноразовый SMS-пароль, который применяется для входа в интернет-банкинг, в целях восстановления пароля либо смены устройства или браузера при получении доступа к аккаунту в сервисе или социальной сети.

Данные подходы продолжают использоваться, но для жизненно важных сфер они уступили место более надежным с позиции достоверности и безопасности решениям. В числе таких стали выступать платформы цифровой идентификации личности с использованием технологии блокчейн. В них часто для идентификации необходима регистрация в приложении и ввод персональных данных; верификация платформой подлинности введенных данных с помощью «третьей стороны» – партнеров (государственные и частные компании), перевод полученной информации в зашифрованный блок, добавление в блокчейн.

Постепенно набирают популярность комплексные идентификационные сервисы «удаленной онлайн-верификации пользователей» на основе концепции «цифрового следа», интегрированные с веб-платформой компании, как, например, это сделано в одном из отечественных сервисов – системе CheckU[6]. Платформа определяет надлежащую идентификацию по фотографии пользователя – пользователь делает «селфи» на смартфон или компьютер, а CheckU распознает, что перед камерой человек, а не фото или видео. При загрузке документа пользователь загружает скан или фото документа, удостоверяющего личность, которые CheckU проверяет на признаки подделки. Обязанность пользователя – предоставить достоверные сведения.

Стоит отметить, что с появлением дополнительных способов защиты устройств от несанкционированного использования, таких, например, как графический ключ или элемент для биометрического распознавания пользователя, сами эти устройства зачастую выполняют роль дополнительного фактора, усиливающего защиту и обеспечивающую более высокий уровень достоверности процесса идентификации. Таким образом, можно говорить о комбинировании различных технологий идентификации. Для социальных сетей, например, Facebook, после регистрации аккаунта пользователь идентифицируется через IP- либо MAC-адрес, номер телефона, устройство либо используемый браузер. Изменение любого из этих параметров приводит к

[6] См.: Подтверждение личности автоматически за 2 минуты. [Электронный ресурс]. URL: https://checku.co/ru/ (дата обращения: 28.02.2020).

необходимости дополнительной аутентификации, которая выполняется через новый ввод зарегистрированного пароля, либо через код, полученный в SMS-сообщении. При настроенной двухфакторной аутентификации пользователю необходимо вводить специальный код для входа или подтверждать вход при каждой попытке получить доступ к аккаунту Facebook с неопознанного компьютера или мобильного устройства. Позиция Facebook заключается в том, что надлежащей идентификацией пользователя является предоставление данных пользователя, т. е. «любых данных, в том числе согласие человека или информация (позволяющая установить личность или анонимная), которую вы или третьи стороны получаете от Facebook или через Facebook» [3]. Обязанность пользователя – предоставить данные, соответствующие действительности.

Примечательно, что схожая логика нашла отражение в Постановлении Правительства Российской Федерации от 27.10.2018 № 1279 «Об утверждении Правил идентификации пользователей информационно-телекоммуникационной сети “Интернет” организатором сервиса обмена мгновенными сообщениями» (далее – Правила), которым были утверждены новые Правила идентификации пользователей в мессенджерах, цель которых установить, что личности владельца SIM-карты и того, кто планирует пользоваться мессенджером, совпадают; при этом оператор сотовой связи должен знать обо всех приложениях для обмена сообщениями, которые использует пользователь. Согласно Правилам, в целях осуществления идентификации абонентский номер, выделенный пользователю сервиса обмена мгновенными сообщениями, предоставляется пользователем сервиса обмена мгновенными сообщениями организатору сервиса обмена мгновенными сообщениями. Для подтверждения абонентского номера организатор сервиса обмена мгновенными сообщениями предлагает пользователю совершить действия с использованием этого абонентского номера, позволяющие достоверно установить, что сообщенный абонентский номер при регистрации в сервисе обмена мгновенными сообщениями используется именно его владельцем.

Наряду с использованием информации об аппаратном и программном обеспечении лиц, широкую конкуренцию им составляют уже упомянутые технологии биометрической идентификации, которые стали неотъемлемым компонентом мирового рынка информационных технологий и становятся удобным инструментом для решения широкого круга задач. В настоящее время они наиболее всего апробированы и востребованы в финансовом секторе, при электронных транзакциях, при распространении пользовательских

абонентских устройств (в первую очередь смартфонов), но наблюдается уверенная тенденция к тому, чтобы распространить их на важнейшие социальные сферы, такие как медицина, образование и социальное обеспечение.

Одним из типов биометрических характеристик являются статические биометрические данные. К ним относятся уникальные признаки, полученные человеком от рождения. Соответственно видом таких биометрических данных будут являться, например, отпечатки пальцев, радужная оболочка глаза, геометрия руки и т.д. Также используются динамические биометрические данные – характеристики, приобретённые со временем или способные меняться с возрастом или под внешним воздействием. К ним можно отнести черты лица (face recognition), радужную оболочку глаза, голос, рисунок вен, геометрию ладони, иное.

Заметим, что этапы биометрической идентификации как для статических, так и для динамических биометрических данных совпадают:

1) запись – система запоминает биометрические данные;

2) выделение биометрического образца – информация обрабатывается и преобразовывается в математический код;

3) сравнение – сохраненный биометрический образец сравнивается с предоставленным в ходе проведения идентификации.

Главной проблемой биометрической идентификации, в первую очередь в отношении статических биометрических данных, выступает тот факт, что биометрическими данными несложно незаконно завладеть и воспользоваться. Например, как только стала популярна технология TouchID от компании Apple (активация смартфона по отпечатку пальца), исследователи из The Chaos Computer Club создали дублирующие пальцевые отпечатки, чтобы взломать устройства и анонсировали факт успешного взлома, используя традиционные способы клонирования пальцевых отпечатков [6].

Последним направлением развития технологий идентификации, имеющим большие перспективы в будущем, является использование генетической информации. В практике многих стран первоначально методы генетической регистрации использовались только в отношении граждан, которые совершали преступления или являлись подозреваемыми в их совершении [7], позже круг субъектов был расширен иными категориями граждан, например, состоящих на государственной службе. На сегодняшний день идентификация по ДНК вышла за пределы уголовно-правового или криминалистического характера.

По мнению И.М. Рассолова, С.Г. Чубукова, И.В. Микурова, «методы анализа ДНК быстро развиваются. По общему признанию, генетические характеристики, содержащиеся в «кодирующих» областях, сохраняются и используются только в медицинских целях или для научных исследований, тогда как генетические отпечатки пальцев, используемые полицией и правосудием, касаются только маркеров пола и идентификации» [5, с. 115].

Вместе с тем, как отмечает С.Н. Кубитович, «с молекулой ДНК, помимо ее индивидуальности, связано и другое основополагающее свойство - наследственность и способ передачи наследственной информации. Таким образом, молекула ДНК является носителем информации не только о конкретном индивидууме, но и о его родителях и родственниках» [2, с. 186]. Принимая во внимание этот факт и анализируя случаи применения идентификации по ДНК, можно говорить о достаточной точности такого метода идентификации.

Однако идентификация по ДНК является очевидно ресурсоёмким, небыстрым и, как следствие, весьма дорогим методом. Высокая рыночная стоимость этого метода складывается из сложности ДНК-технологий при проведении научных опытов и массовых ДНК-скринингов населения. Создание так называемого «генетического паспорта» субъекта идентификации пока крайне затратно, но очевидно, что при удешевлении соответствующих технологий надлежащие способы идентификации могут стать массовыми.

Подводя итоги проведенному обзору и анализу существующих популярных коммерческих систем идентификации, можно еще раз подчеркнуть зависимость правовых аспектов идентификации от природы и свойств используемых технологий. При этом во всех сферах и примерах идентификация представляет собой информационный процесс, где наибольший интерес представляет установление состава участников правоотношений.

Результатом идентификации, проводимой путем использования различного вида идентификаторов и сравнения информации о субъекте или объекте с имеющейся информацией о них в той или иной информационной системе, является юридический факт, с учетом содержания которого у лиц возникают те или иные права и обязанности в различных правоотношениях.

Несмотря на то что понятие идентификации и идентификатора теперь часто встречается в законодательстве, в законе до сих пор отсутствует их единое правовое определение, и различные отрасли права давно начали оперировать собственным содержанием данных терминов, что недопустимо и требует скорейшей гармонизации предметной терминологии.

Отдельного правового закрепления в законе требует система понятий, связанных с инфраструктурой идентификации с раскрытием видов субъектов, объектов и реализуемых с помощью последних функций. Субъекты, участвующие в идентификации, выполняют различные задачи, могут иметь различные интересы, при этом используемые ими технологии могут не быть надежными. И здесь возникает принципиальная проблема обеспечения безопасности и достоверности идентификации, которая в перспективе может потребовать введения новых контролирующих функций у государства, а также установления юридической ответственности лиц за правонарушения, связанные с недостоверной и/или незаконной идентификацией.

Список литературы

1. В России создадут цифровой профиль гражданина // Рос. газета. – № 44 (7802) от 27.02.2019.

2. Кубитович С. Н. ДНК как носитель информации неограниченного круга лиц // Вестн. экон. безопасности. – 2017. – № 4. – С. 185–190.

3. Официальный сайт Facebook. Политика платформы. [Электронный ресурс]. – URL: https://developers.facebook.com/policy (дата обращения: 29.02.2020).

4. Портал государственных услуг. Официальный сайт. Вход и регистрация. [Электронный ресурс]. – URL: https://www.gosuslugi.ru/help/faq/c-1 (дата обращения: 29.02.2020).

5. Рассолов И.М., Чубуков С.Г., Микуров И.В. Биометрия в контексте персональных данных и генетической информации: правовые проблемы // Lex Russia (Русский закон). – 2019. – № 1 (146). – С. 108–118.

6. Chaos Computer Club claims it can unlock Iphones with fake fingers/cloned fingerprints. [Электронный ресурс]. – URL: https://boingboing.net/2013/09/22/chaos-computer-club-claims-it.html (дата обращения: 29.02.2020).

7. Criminal Justice and Police Act 2001. [Электронный ресурс]. – URL: http://www.legislation.gov.uk/ukpga/2001/16/section/82 (дата обращения: 18.02.2020).

8. OpenID Foundation website. [Электронный ресурс]. – URL: https://openid.net/ (дата обращения: 28.02.2020).

Статья поступила 03.03.2020 г.