МИНИСТЕРСВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САМАРСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА С.П. КОРОЛЕВА»
(САМАРСКИЙ УНИВЕРСИТЕТ)

В. Э. ВОЛКОВ

ЦИФРОВОЕ ПРАВО. ОБЩАЯ ЧАСТЬ

Рекомендовано редакционно-издательским советом федерального государственного автономного образовательного учреждения высшего образования «Самарский национальный исследовательский университет имени академика С.П. Королева» в качестве учебного пособия для обучающихся по основным образовательным программам высшего образования по направлениям подготовки 40.03.01, 40.04.01 Юриспруденция

Самара
Издательство Самарского университета
2022

УДК 342.7(075)
ББК 67.400.3я7
В676

Рецензенты:
Юдин Андрей Владимирович – доктор юридических наук, профессор, заведующий кафедрой гражданского процессуального и предпринимательского права ФГБОУ ВО «Самарский национальный исследовательский университет имени академика С.П. Королева»;
Михайлова Наталья Александровна – Руководитель Управления Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Самарской области

Волков, Владислав Эдуардович
В676 Цифровое право. Общая часть: учебное пособие / *В. Э. Волков.* – Самара: Издательство Самарского университета, 2022. – 111 с.

ISBN 978-5-7883-1770-0

Учебное пособие содержит комплексный анализ правового режима цифровой информации. Автором пособия рассмотрены правовые и социальные основания регулирования отношений, связанных с оборотом цифровых данных и применением цифровых информационных технологий, подходы к определению субъектов соответствующих правоотношений, а также субъективные права на поиск, получение, предоставление и распространение информации в цифровой форме.

Учебное пособие ориентировано на широкий круг читателей, включая студентов и преподавателей высших учебных заведений, юристов, работников органов публичной власти.

УДК 342.7(075)
ББК 67.400.3я7

ISBN 978-5-7883-1770-0

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ

Разговор о праве сегодня принято начинать с утверждений о неизбежности скорой цифровой революции, которая принесет нам неисчислимые блага – освобождение от рутины, повышение качества жизни, а в перспективе, может быть, и безусловный доход. Позволю себе с этим не согласиться. Ожидания цифровой революции безосновательны. Она уже состоялась. Мы уже перешли к новому цифровому укладу и сейчас находимся в прекрасном новом цифровом мире.

Даже такой консервативный общественный институт, как система образования, подвергся цифровой трансформации, и сейчас мы с вами общаемся в цифровой среде. Она не просто создала большие возможности доступа к знаниям, но и изменила роль участников обучения. Теперь не студент является в аудиторию к преподавателю, а сам преподаватель приходит к студенту, где бы студент ни находился. В этой ситуации баланс внимания смещается от учителя к ученику. Он принимает своей волей и в своем интересе решение – позволить ли преподавателю принять участие в формировании своей картины мира и если да, то предоставляет в распоряжение преподавателя один из наиболее ценных ресурсов цифровой экономики – свое внимание. Благодарю вас за эту возможность!

При подготовке пособия автор ориентировался на методологические подходы к анализу существующих правовых явлений, сформулированные на кафедре государственного и административного права Самарского университета под руководством заведующего кафедрой профессора Виктора Владимировича Полянского.

ГЛАВА I. ПРАВОВЫЕ ОСНОВАНИЯ РЕГУЛИРОВАНИЯ ЦИФРОВЫХ ОТНОШЕНИЙ

1.1. Понятие цифрового права

В современном мире не только состоялась цифровая революция, но и происходит реставрация дореволюционных порядков, правда тоже в цифровой форме. В ответ на цифровую глобализацию государства пытаются приспособить традиционные юридические механизмы к условиям нового мирового порядка. Какими будут государство и право в новом цифровом мире? Ни российское, ни мировое юридическое сообщество пока не нашли ответ на этот вопрос. Право отличается естественным консерватизмом и стабильностью. Неизменность правового акта, применение его в течение длительного времени являются его позитивными юридическими свойствами. Причем чем выше юридическая сила акта, тем большая стабильность ему придается. Например, в большинстве государств конституция действует в неизменном виде длительное время и не требует внесения поправок, а изменение Конституции всегда становится событием общенационального масштаба.

Цифровая реальность развивается по другой логике, имеющей преимущественно экономическую и технологическую природу. Мы затронем некоторые аспекты цифровой экономики в дальнейшем, но уже сейчас надо отметить, что законы государства не «успевают» за цифровыми технологиями, работающими по своим собственным правилам. Таким, как Закон Мура, согласно современной интерпретации которого, производительность процессоров удваивается каждые 18 месяцев[1]. Или Закон Эдхольма, который предсказывает, что

[1] Exponential Laws of Computing Growth. By Peter J. Denning, Ted G. Lewis. Communications of the ACM, January 2017. – Vol. 60. – № 1. – P. 54-65.

каждые 18 месяцев удваивается пропускная способность передачи данных в компьютерных сетях. Закон Эдхольма проявляется везде, где передача данных обеспечивается применением цифровых технологий[2]. Увеличение объема цифровой информации объективно должно привести к росту объема задач, стоящих перед правовой системой. Однако даже поверхностный анализ состояния правотворчества и правоприменения показывает, что ни объем нормативного материала, ни качество его реализации не увеличиваются такими темпами.

Для решения проблемы отставания права от потребностей цифровой среды юридическим сообществом предложены два основных направления. Первый состоит в формировании совершенно нового правопонимания и цифровой правовой культуры, второй – в приспособлении уже имеющихся правовых институтов к цифровой реальности. Их реализация в юридической теории и практике приводит к определению цифрового права в широком и узком значениях.

В широком смысле цифровое право понимается как новый нормативный правовой механизм, затрагивающий любой элемент правовой системы. Широкий подход основан на очевидном факте, что правовые нормы – это тоже информация. Информация о правах, обязанностях, об их реализации. Регулируя общественные отношения, право регулирует и само себя, приобретая новый смысл и новое значение, когда общение между людьми приобретает цифровую форму. Уникальные особенности цифровой информации – нематериальность, техническая обусловленность, медиатизация в сочетании с высоким спросом на нее, требуют уникальных правовых решений.

В рамках данного подхода любое правовое регулирование независимо от его отраслевой принадлежности рассматривается как

---

[2] Cherry S. Edholm's law of bandwidth // IEEE Spectrum. – Vol. 41. – № 7. – P. 58-60. July 2004, doi: 10.1109/MSPEC.2004.1309810.

имеющее информационную и преимущественно цифровую природу. Принципиальная возможность перевода правовых отношений в форму цифрового взаимодействия сегодня уже не вызывает сомнений. Система электронного взаимодействия уже успешно применяется для оказания государственных услуг, в арбитражном процессе, при подаче заявок на регистрацию товарных знаков и в других сферах.

Цифровое право в широком смысле не предполагает выделение особой отрасли права или правового института, а скорее представляет собой новое направление государственного регулирования цифровой реальности. Оно способно в перспективе заново отформатировать правовую систему и предложить вместо нынешнего деления правовой системы на отрасли что-то совершенно новое. Например, деление права на «цифровое» и «аналоговое» или «фундаментальное» и «прикладное». Причем последний вариант, предложенный авторами учебника по цифровому праву под редакцией В.В. Блажеева и М.А. Егоровой, даже предполагает выход за пределы формального права и ведущую роль «массового правового сознания населения, которое живет в автономном режиме от формальных регуляторов и не стремится видеть в формальном праве часть своей повседневности»[3]. Проявление этого подхода можно видеть уже сейчас в отношении общества к государственному регулированию сети «Интернет». Интернет не без оснований рассматривается его пользователями как пространство разума и свободы, основанное на общечеловеческих ценностях, а не на позитивном формальном праве. Меры, направленные на ограничение общения в сети, особенно если они касаются «неудобной» для властей информации, зачастую оцениваются как нелегитимные и причиняющие гражданам необоснованные неудобства.

---

[3] Цифровое право: учебник / А. Дюфло, Л.В. Андреева, В.В. Блажеев [и др.]; под общ. ред. В.В. Блажеева, М.А. Егоровой. – М.: Проспект, 2020. – 640 с.

Несколько визионерский характер широкого подхода к цифровому праву не отменяет его продуктивности для формирования представления о судьбе права в недалеком цифровом будущем. Широкий подход является основанием для выделения своего рода «общей части» цифрового права, охватывающей отношения по поводу регулирования цифровой информации независимо от ее отраслевой принадлежности. Ведущая роль в ней принадлежит юридическим характеристикам цифровых данных и цифровых технологий, изучению которых посвящен наш курс.

Более формальным, направленным на практическое решение актуальных проблем с помощью уже существующих правовых институтов, является понимание цифрового права как комплексного межотраслевого правового института. Системообразующим принципом для объединения его норм является сфера государственного управления, сложившаяся в результате цифровой трансформации.

Комплексный межотраслевой правовой институт – это вторичное правовое образование, в котором по предметному, тематическому или целевому признаку объединен разнородный правовой материал. Цифровое право в данном случае понимается как комплексный правовой институт, состоящий из действующих правовых норм, регулирующих отношения, связанные с поиском, получением, передачей, производством и распространением цифровых данных, а также с применением цифровых информационных технологий. Эти нормы находятся в документах разной отраслевой принадлежности и подчиняются различной юридической методологии. Например, регулирование технологий искусственного интеллекта требует одновременной реализации как норм публичного права для обеспечения безопасности, гарантий прав и свобод человека, защиты персональных данных, так и частно-правовых норм, направленных на защиту имущественных интересов, интеллектуальных

прав, возмещения вреда, причиненного с применением технологий искусственного интеллекта.

Цифровое право как в широком, так и в узком смысле, имеет уникальный субъектно-объектный состав. Многие участники цифровых отношений не осознавались в качестве носителей прав и обязанностей еще несколько лет назад. Выдвигаются смелые предположения о наделении правами и обязанностями неодушевленных сущностей, функционирующих на основе технологий робототехники и искусственного интеллекта – «цифровых сущностей». Другие субъекты, едва получив правовое признание, уже успели его утратить. Например, специальное правовое регулирование деятельности блогеров просуществовало всего 3 года – с 2013 по 2017 год.

Традиционные для классического «аналогового» права субъекты – граждане и их объединения – уже приобрели новые правовые возможности – право на забвение, право на цифровую смерть, право на анонимность в сетевых отношениях, защиту цифровых персональных данных и т.д. Очевидно, что осознание и законодательное закрепление новых правовых возможностей в цифровом мире будет продолжено.

Цифровое право в узком значении как комплексный межотраслевой правовой институт служит целям регулирования отношений, связанных с реализацией существующих цифровых технологий. Согласно паспорту национальной программы «Цифровая экономика России» к цифровым технологиям, имеющим наибольшее значение для государства и, следовательно, подлежащим правовому регулированию, отнесены:

- нейротехнологии и искусственный интеллект;
- технологии виртуальной и дополненной реальности;
- технологии распределенного реестра;
- квантовые технологии;
- новые производственные технологии;

- компоненты робототехники и сенсорика;
- технологии беспроводной связи.

Реализация каждой технологии требует новых правовых решений. Сочетание широкого и узкого подхода к цифровому праву позволяет поставить перспективную задачу его определения как новой комплексной отрасли права. Для ее решения правовой материал, находящийся в сфере цифрового права может быть разделен на общую и специальную часть. Назначение общей части цифрового права видится в обеспечении отрасли общими принципами, методологией и категориальным аппаратом. В свою очередь, быстрое развитие прикладных технологий означает необходимость формирования правовых институтов, обеспечивающих применение конкретных цифровых технологий и образующих специальную часть цифрового права.

Сказанное позволяет определить цифровое право в широком смысле как новое направление правового регулирования, правовой механизм, обеспечивающий развитие цифрового общества. В узком смысле цифровое право – это комплексный межотраслевой правовой институт, объединяющий нормы основных отраслей права, регулирующие отношения, связанные с поиском, получением, передачей, производством и распространением цифровых данных, а также с применением цифровых информационных технологий.

1.2. Цифровая информация как объект регулирования: медиатизация и цифровая форма

Независимо от подходов, применяемых для определения цифрового права, объектом его регулирования является информация, представленная в цифровой форме. В России для регулирования информационных отношений принят специальный Федеральный закон «Об информации, информационных технологиях и защите ин-

формации» от 27 июля 2006 г. № 149-ФЗ[4] (далее – Закон об информации). Информация имеет многочисленные формы выражения и поэтому в законе определена неоднозначно. Согласно ст. 2. закона информация – это сведения (сообщения, данные) независимо от формы их представления. Таким образом, описание информации как сведений дополнено интерпретацией: в коммуникационном смысле – в форме сообщений, в техническом смысле – в форме данных. Это позволяет обратить внимание на два юридически значимых признака цифровой информации.

Во-первых, цифровая информация обычно воспринимается человеком не сама по себе, а в составе какого-то технического решения, позволяющего перевести ее с языка цифр и передать по каналам связи. Иными словами, современное право «замечает» цифровую информацию, только когда она участвует в коммуникации через медиа (посредника), которым может быть какой-либо носитель цифровой информации (жесткий диск компьютера, флэш-накопитель), техническое устройство (оперативная память ЭВМ) или физическая среда (например, электромагнитные импульсы). Это несколько упрощает задачу регламентации цифровых отношений в сравнении с аналоговыми. Аналоговый сигнал часто является немедиатизированным и неуловимым для государственного регулирования. Например, процессуальная ситуация «слово против слова», когда у сторон нет других оснований для взаимных претензий, кроме произнесенных в прошлом и не зафиксированных слов, является трудноразрешимой с формально юридической точки зрения.

[4] Федеральный закон «Об информации, информационных технологиях и защите информации» от 27 июля 2006 г. № 149-ФЗ // Собрание законодательства РФ. – 2006. – 31 июля. – № 31 (1 ч.). – Ст. 3448.

Медиатизация означает, что необходимым элементом отношений с участием цифровой информации является определенная техническая система. Например, при определении оптимальных способов регулирования Интернета необходимо учитывать его децентрализованную сетевую структуру, наличие в ней различных по своему предназначению слоев модели OSI[5], а иначе либо регулирование окажется неэффективными, либо Интернету как ценности будет нанесен вред. Поэтому действие норм цифрового права должно сочетаться с пониманием и соблюдением технологических норм, которые сами по себе имеют значительный регулятивный ресурс и в ряде случаев могут рассматриваться как альтернатива юридическим регуляторам либо их дополнение. Так, чисто технические решения, блокирующие один из протоколов всемирной сети – UDP, могут, в принципе, снять проблему регулирования информации, передаваемой через торрент-сети. Блокировка UDP сделает торрент-сеть фактически неработоспособной. Это исключит необходимость юридической квалификации содержания передаваемой с ее помощью информации. Правда, и полноценного Интернета тогда тоже не будет. Что происходит в случае игнорирования особенностей медиасреды уважаемые читатели наверняка знают на примере ограничения доступа к Telegram в 2018 году. Попытки Роскомнадзора заблокировать трафик мессенджера привели к отказам многочисленных ресурсов, не имеющих отношения к спору государственного регулятора с Telegram.

Использование особой технической инфраструктуры передачи цифровой информации также приводит к необходимости наделения особыми правами и обязанностями информационных посредников –

[5] Подробнее о модели OSI и ее влиянии на правовое регулирование сетевых отношений см.: Solum, Lawrence B. and Chung, Minn, The Layers Principle: Internet Architecture and the Law. – URL: https://ssrn.com/abstract=416263 (дата обращения 01.12.22).

лиц и организаций, обеспечивающих передачу данных в сети и доступ к ее ресурсам – провайдеров доступа к сети, провайдеров хостинга, поисковых систем, новостных агрегаторов, социальных сетей и т.д. Особенностям их правового статуса посвящен параграф 3.2.

Вторым важным свойством цифровой информации является ее представление в форме данных. Цифровые данные – это информация, представленная в виде дискретных символов, каждый из которых может принимать одно из конечного числа значений некоторого алфавита, например буквы или цифры. Наиболее распространенной формой цифровых данных являются двоичные данные, которые представлены строкой двоичных цифр (битов), каждая из которых может иметь одно из двух значений: 0 или 1.

Сведения, представленные в цифровой форме, на современном уровне развития техники приобретают особую ценность в силу возможности их автоматизированной обработки и использования как необходимого ресурса для реализации цифровых технологий. В частности, наличие большого количества качественных структурированных цифровых данных является критически важным для систем искусственного интеллекта. Их реализация, в свою очередь, обеспечивает исключительно высокий уровень прибавочной стоимости цифровых активов, недостижимый для продуктов доцифровой экономики. Поэтому распространено образное восприятие цифровых данных как топлива для новой экономики.

Повышенный спрос на цифровые данные, требует реализации правовых мер, направленных на их защиту. В частности, особой защиты требуют персональные цифровые данные граждан России. Для соотечественников традиционно характерен несколько завышенный в сравнении с гражданами стран Европы и Северной Америки уровень технооптимизма, не подкрепленный пониманием закономерностей развития цифровой информационной среде. Резуль-

таты социологических исследований показывают, что каждый второй из опрошенных пользователей (49%) готов предоставлять какую-либо личную информацию, если понимает цели ее использования и разделяет их важность, при этом лишь пятая часть пользуются программами, которые ограничивают возможность отслеживать действия в сети. Для придания цифровой информации юридически значимой формы требуется применение специальных правовых конструкций – электронное сообщение и электронный документ. Электронный документ является частным случаем электронного сообщения и характеризуется: а) возможностью восприятия человеком содержания информации; б) наличием определенных реквизитов, позволяющих определить информацию или в установленных законодательством случаях – ее материальный носитель[6]. Отличия электронного документа от обычного (бумажного) определяются его видом – он представляет собой последовательность дискретных символов (байтов), находящихся в памяти ЭВМ или другого запоминающего устройства. Они нематериальны, могут быть легко заменены на другие или удалены, для их непосредственного восприятия человеком требуются либо специальные знания (например, языков программирования) или технические устройства. В связи с этим для полноценного включения электронных документов в правовую среду требуется «перевод» электронного документа с машинного языка на язык, воспринимаемый человеком, и обратно.

Сторонники полной цифровизации документооборота допускают вариант, когда этого не требуется и, например, машинный код, на котором изложен смарт-контракт рассматривается как язык изложения текста договора по аналогии с иностранным языком. Эта

[6] См. Савельев А. И. Комментарий к Федеральному закону от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» (постатейный). – М.: Статут, 2015.

точка зрения требует серьезной проработки и вряд ли может быть уже сейчас принята в качестве руководства к действию.

Во-первых, код электронного документа может быть выражен как на языке программирования (например, на Solidity) так и в байт-коде. Байт-код – результат трансляции языка программирования при выполнении смарт-контракта в последовательности символов – команд для процессора. Эта последовательность практически недоступна для интерпретации человеком. Возможность выражения юридически значимых документов в текстах, недоступных для человеческого понимания пока представляется преждевременной.

Во-вторых, даже если допустить, что язык электронного документа – это не байт-код, а какой-либо известный человечеству язык программирования, то проблема перевода также не решена. Уровень распространенности цифровых знаний не дает оснований для обоснованного расчета на то, что содержание правоотношений, опосредованных такой цифровой формой, будет осознано каждым субъектом правоотношений. На преждевременность полной цифровизации документооборота указывает и содержание российского законодательства – согласно статье 160 Гражданского кодекса Российской Федерации сделка, заключенная с помощью электронных или иных технических средств считается заключенной только если эти средства позволяют воспроизвести на материальном носителе в неизменном виде содержание сделки. Таким образом действующее гражданское законодательство предусматривает обязательный «перевод» машинного языка электронного документа на язык человека. Это может быть сделано путем отображения содержания сделки на мониторе компьютера, путем печати бумажного документа и т.д.

Кроме того, в качестве реквизита электронного сообщения, достаточного для придания ему статуса электронного документа, может выступать электронная подпись или иной аналог собственноручной подписи, признаваемый законом или договором. Вопросы

идентификации и аутентификации субъектов цифровых отношений будут рассмотрены в параграфе 3.3.

1.3. Цифровая информация как объект регулирования: идеальность, неисчерпаемость и субъективность восприятия

Помимо медиатизации и формы представления цифровые данные также обладают юридическими свойствами, присущими любой информации.

Информация нематериальна, она может находиться одновременно в ведении многих лиц. В силу этого к ней неприменимы правовые конструкции, основанные на физическом держании и отчуждении материального объекта. В частности, в отношении информации невозможно осуществление права владения, что в условиях российской цивилистической доктрины исключает реализацию в отношении нее права собственности. В соответствии с концепцией, получившей развитие в информационном законодательстве России, граждане, юридические лица, публичные образования могут быть не собственниками, а обладателями информации. Неприменимость в отношении информации идеологии права собственности привела к формированию новых частноправовых институтов, одним из которых являются «цифровые права», предусмотренные Федеральным законом от 18 марта 2019 г. № 34-ФЗ[7].

Другим свойством информации является ее неисчерпаемость. Неподверженность цифровых данных физическому старению приводит к образованию огромных массивов информации, одновременно доступных фактически неограниченному кругу лиц, к тому

[7] Федеральный закон от 18.03.2019 № 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации» // Собрание законодательства Российской Федерации. – 2019. – № 12. – Ст. 1224.

же находящихся в разных юрисдикциях. Это свойство цифровой информации оказывает деструктивное влияние на «аналоговые» правовые институты. Так, цифровая дистрибуция контента, бурное развитие социальных сетей, аудиовизуальных сервисов привели к неэффективности ограничений массовой информации, предусмотренных законодательством о СМИ. Классические СМИ вынуждены соблюдать правила, неведомые основным распространителям массовой информации в сети, которыми сегодня являются аудиовизуальные сервисы и социальные сети. Легкость и дешевизна копирования цифровой информации требует новых правовых решений для защиты информации ограниченного доступа и новой методологии подтверждения авторства на результаты интеллектуальной деятельности.

Еще в 2006 году объем медиапотребления среднего американского подростка составлял 30 часов в день. На первый взгляд это невозможно. Но современная жизнь позволяет одновременно получать информацию из различных источников, например, слушать лекцию, листая при этом Инстаграм. Есть основания предполагать, что уровень медиапотребления с 2006 года существенно возрос и не только в США. Накопление больших объемов цифровой информации и ограниченность биологических возможностей человека по ее восприятию информации привели к распространению поисковых и рекомендательных систем. С одной стороны, рекомендательные системы облегчают получение информации, но с другой, разрывают (фрагментируют) целостное информационное поле на сегменты, привлекательные для каждого отдельного потребителя. Они помещают каждого человека в уникальное для каждого информационное пространство, названное в публицистике «пузырем фильтров»[8]. Его

[8] Eli Pariser. The Filter Bubble: What The Internet Is Hiding From You. Penguin UK, 2011.

характерные элементы – алгоритмические ленты в социальных сетях вместо хронологических, рекомендации аудиовизуальных сервисов и т.д. Определяющее значение поисковых систем для формирования картины мира требует возложения на них и дополнительных обязанностей, например, связанных с реализацией права на забвение.

Последним по порядку, но не по значению является свойство информации, заключающееся в субъективности ее восприятия. Ценность информации определяется самим потребителем. Причем для разных потребителей одна и та же информация может обладать разной ценностью. На оценку информации влияют потребность в информации, наличие у потребителя компетенций, равно как и барьеров для ее восприятия. Например, простое знание иностранного языка может существенно повысить качество жизни в цифровой среде, поскольку цифровые технологии имеют глобальных характер и документируются как правило на английском языке. Многие современные технологии цифровой дистрибуции основаны на проявлении субъективного отношения к информации и стимулируют социальное разобщение (таргетирование) для продвижения товаров и услуг на рынке. Современная цифровая экономика практически исключает возможность существования ценностей, разделяемых всеми членами общества. Сложившаяся ситуация помимо решения стратегической задачи поддержания социальной солидарности делает актуальными прикладные задачи правоприменения. В частности, определение лица, ответственного за деятельность алгоритмов, формирующих информационную повестку (Яндекс Новости, Google News, рекомендательная система YouTube и т.д.). Кто несет юридическую ответственность за то, что YouTube предлагает посмотреть агитационный ролик, в день, когда агитация запрещена? Пока на этот вопрос нет определенного ответа.

Учет перечисленных признаков цифровой информации – идеальности, неисчерпаемости и субъективности восприятия – имеет определяющее значение для успеха правового регулирования цифровой трансформации.

1.4. Действие норм цифрового права в пространстве

Оборот цифровых данных оказывает существенное влияние на понимание суверенитета современных государств. Технологии имеют глобальный характер, а современное право пока еще говорит на государственном языке той или иной страны. Право предназначено для защиты не глобальных, а национальных ценностей, свойственных народу конкретного государства. Между цифровыми технологиями и государственным правопорядком объективно существует напряженность. Попытки ее устранения вызывают к жизни новые правовые решения.

Интервенция глобальных цифровых технологий в правопорядок суверенных государств требует определения новых параметров действия права в пространстве. Действие норм права обычно имеет территориальный характер и распространяется на географическое пространство внутри государственных границ. Тогда как сетевые информационных технологии интернациональны. Они пригодны для использования любым человеком, где бы он ни находился. Технологии формируют новую реальность в которой человек может одновременно находится в сфере действия разных правовых систем – системы государства, в котором физически находится и системы той страны, по законам которой работает компания, предоставляющая ему то или иное цифровое благо.

В России с 2012 года предпринимаются меры для определения части цифрового пространства, где действует российское право. Начало суверенного Интернета было положено документами орга-

нов исполнительной власти – Письмом Федеральной антимонопольной службы от 13 сентября 2012 г. о требованиях к рекламе алкоголя и Разъяснением Минкомсвязи России о сфере действия Федерального закона «О персональных данных» по территории и кругу лиц. Они определяли признаки, свидетельствующие о направленности интернет-сайта на территорию России. Во-первых? это было использование доменного имени, связанного с Российской Федерацией или субъектом РФ (.ru, .рф., .su, .москва., moscow и т.п.). И во-вторых, наличие русскоязычной версии интернет-сайта. При этом поскольку русский язык широко используется в некоторых странах за пределами Российской Федерации, для определения направленности интернет-сайта именно на территорию Российской Федерации дополнительно требовалось наличие как минимум одного из следующих элементов: возможности осуществления расчетов в российских рублях; возможности исполнения заключенного на таком интернет-сайте договора на территории Российской Федерации (доставки товара, оказания услуги или пользования цифровым контентом на территории России), использование рекламы на русском языке, отсылающей к соответствующему интернет-сайту, или иных обстоятельств, явно свидетельствующих о намерении владельца интернет-сайта включить российский рынок в свою бизнес-стратегию[9].

Указанные акты определили развитие концепции суверенного цифрового пространства России на несколько лет. Но имели очень узкую сферу регулирования и применялись в основном по аналогии. Практика выявила невысокий уровень их реализации. Это было связано в основном с невозможностью их принудительного осуществления как в юридическом, так и в технологическом смысле. Еще не были

[9] Обработка и хранение персональных данных в РФ. Изменения с 1 сентября 2015 года. – URL: https://digital.gov.ru/ru/personaldata/ (дата обращения: 01.02.22).

внедрены технические решения, позволяющие эффективно фильтровать и ограничивать интернет-траффик, поступающий в Россию.

Реализация концепции цифровой территории России вышла на качественно новый уровень с принятием Федерального закона «О деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации» от 1 июля 2021 г. № 236-ФЗ[10]. Этот акт также известен как Закон о приземлении ИТ-компаний. Он по-новому определяет условия, при которых деятельность лица – владельца информационного ресурса считается осуществленной на территории Российской Федерации и подпадающей под действие российского права. Причем под интернет ресурсом теперь понимается не только сайт, но и отдельная страница сайта, информационная система и программа для ЭВМ, например, мобильное приложение.

Для признания деятельности иностранного лица осуществленной на цифровой территории Российской Федерации по закону требуется установление двух критериев: количественного и функционального.

Количественный критерий означает доступ к информационному ресурсу в течение суток более пятисот тысяч пользователей, находящихся на территории России.

Для соблюдения функционального критерия достаточно выполнения любого из следующих условий:

1. Наличие на ресурсе информации на государственном языке Российской Федерации, государственных языках республик в составе Российской Федерации или иных языках народов Российской Федерации. Как видим, требования к языку информационного ресурса были уточнены – если ранее учитывалась только русскоязычная версия, теперь перечень языков существенно расширен.

---

[10] Собрание законодательства РФ. – 2021. – 5 июля. – № 27 (часть I). – Ст. 5064.

2. Распространение рекламы, направленной на привлечение внимания потребителей, находящихся на территории Российской Федерации.

3. Обработка сведений о пользователях, находящихся на территории Российской Федерации. Включение этого нового признака произошло в связи с осознанием особой ценности персональных данных и производных от них сведений для цифровой экономики.

4. Получение денежных средств от российских физических и юридических лиц.

Законом особо определяются лица, которые признаются действующими в цифровом пространстве России независимо от численности аудитории:

- лицо, являющееся провайдером хостинга или иным лицом, обеспечивающим размещение информационных ресурсов в сети «Интернет», пользователи которых находятся в том числе на территории Российской Федерации;
- лицо, осуществляющее деятельность по обеспечению функционирования информационной системы и (или) программы для электронных вычислительных машин, которые предназначены и используются для организации распространения в сети «Интернет» рекламы, направленной на привлечение внимания потребителей, находящихся в том числе на территории Российской Федерации, посредством принадлежащих третьим лицам информационных ресурсов (оператор рекламной системы);
- лицо, осуществляющее деятельность по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети «Интернет», в том числе находящихся на территории Российской Федерации (организатор распространения информации в сети «Интернет»).

Иностранные лица, находящиеся на цифровой территории России обязаны создать уполномоченное юридическое лицо. Также необходимо зарегистрировать личный кабинет на сайте Роскомнадзора, разместить на своем ресурсе электронную форму для обратной связи с российскими гражданами или организациями. Закон также предусматривает меры «понуждения» для иностранных лиц вплоть до полной блокировки ресурсов на территории России. Эффективность норм закона о приземлении еще предстоит оценить, но опыт государств с сходными политическими режимами и уровнем развития технологий, в частности, Турции, дает сторонникам суверенизации Интернета повод для осторожного оптимизма.

Закон о приземлении принят в развитие другого акта, важного для понимания концепции цифровой территории – Федерального закона «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации» от 1 мая 2019 года № 90-ФЗ[11]. В публицистике этот закон также известен как Закон о суверенном интернете или Закон об изоляции Рунета. Он обязал операторов связи установить в их сетях технические средств противодействия угрозам (ТСПУ), которые обеспечивают ограничение доступа к ресурсам Интернета, не соответствующим законодательству России. До вступления закона в силу фильтрация осуществлялась самими провайдерами на основании распоряжений Роскомнадзора. Сегодня в соответствии с законом её в автоматическом режиме обеспечивает оборудование, установленное государством. Роскомнадзор централизованно координирует работу ТСПУ.

По состоянию на конец 2021 года 100% мобильных операторов и около 70% операторов стационарной связи соблюдают требования закона о суверенном интернете. Его действие можно оценить по

[11] Собрание законодательства РФ. 2019. – 6 мая. – № 18. – Ст. 2214.

эффективным мерам замедления Twitter и блокирования информации об «Умном голосовании» во время кампании по выборам депутатов Государственной Думы 2021 года.

На суверенизацию интернет-отношений также направлена норма статьи 15.8 Федерального закона «Об информации…». Она введена Федеральным законом от 29 июля 2017 г. № 276-ФЗ, который в интернет-среде более известен как Закон об анонимайзерах. Норма запрещает предоставлять возможность использования на территории РФ информационно-телекоммуникационных сетей и информационных ресурсов (так называемых анонимайзеров) для получения доступа к информации, доступ к которым ограничен на территории РФ.

Роскомнадзор, по обращению уполномоченных федеральных органов исполнительной власти, определяет работающие анонимайзеры. К ним обычно относятся и VPN (виртуальные частные сети), поэтому критически настроенные пользователи называют этот правовой акт также Законом о запрете VPN. Выявленным анонимайзерам направляется требование о подключении к Федеральной государственной информационной системе (ФГИС), содержащей реестр запрещенных сайтов. Подключение к данной системе подразумевает дальнейший запрет выдавать пользователям доступ к сайтам, которые были признаны запрещенными на территории РФ. Если владелец анонимайзера не сделал этого в течение 30 дней с момента получения требования, его работа блокируется Роскомнадзором. На основании указанной нормы в 2021 году в России ограничена работа популярных VPN- и прокси-сервисов RedShieldVPN, OperaVPN, Hola!VPN, TunnelBear, ExpressVPN и др.

Технологии виртуальных частных сетей используются в инфраструктуре многих легальных бизнес-процессов, запрет их использования приведет к несоразмерным потерям для цифровой эко-

номики. Поэтому особенность российского регулирования анонимайзеров состоит в формировании белых списков VPN-сервисов, соблюдающих законодательство России и не подвергающихся блокировкам. В связи с этим утверждение о полном запрете в России VPN как технологии является преувеличением.

Сходный по смыслу Федеральный закон от 27.06.2018 № 155-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»[12] дополнил КоАП статьей 13.40 «Неисполнение обязанностей оператором поисковой системы». Она предусматривает административное наказание в виде штрафа для операторов поисковых систем за выдачу ссылок на заблокированные информационные ресурсы.

Закон устанавливает следующую процедуру. Операторы поисковых систем (как ранее анонимайзеры) обязаны подключиться к ФГИС, содержащей реестр запрещенных сайтов. Если оператор поисковой системы не подключился к ФГИС и не прекратил выдачу ссылок на запрещенные сайты на него может быть наложен штраф (до 700 тыс. рублей для юридических лиц).

Объективные сложности в определении суверенного цифрового пространства приводит современные государства к другой крайности – применению национальных правовых механизмов за пределами государственных границ. В частности, при разрешении дел, связанных с реализацией так называемого права на забвение, французский регулятор обязывал Google исключить определенные ссылки и результаты поисковой выдачи не только на территории Франции, но и во всем мире. Подобная трансляция национальных правовых норм в глобальное информационное пространство вызывает не меньшие возражения, чем попытки огораживания суверен-

[12] Собрание законодательства РФ. – 2018. – 2 июля. – № 27. – Ст. 3938.

ных сегментов Интернета. Нормы национального права оказываются обязательными не только для граждан соответствующего государства, но и для всех остальных пользователей Интернета. Оценим последствия выполнение требований французского регулятора в отношении поисковой выдачи, демонстрируемой, например, гражданам России. Оно приведет к тому, что право российского гражданина на поиск и получение информации будет ограничено решением зарубежного органа власти, принятого в зарубежной юрисдикции на основании зарубежных правовых норм. Такое положение столь же разрушительно для концепции территориального суверенитета, как и неспособность государств контролировать трансграничные информационные потоки.

1.5. Действие норм цифрового права во времени

Цифровая коммуникация меняет восприятие не только пространства, но и времени. В сетевых сообществах время локализуется внутри них и воспринимается как длительность процесса, а не как природный цикл. Виртуальные миры имеют свое собственное время, асинхронное с реальным пространством. При этом временные характеристики имеют существенное значение для реализации правовых норм. Обычно это укладывается в последовательность юридических событий и действий. Хронология определяет процессуальный порядок реализации многих правовых институтов. В том числе значимых для цифровой экономики, таких как свобода слова, права на поиск, получение, передачу, производство и распространение информации.

Информационные технологии сегодняшнего дня благодаря существенно расширившимся возможностям хранения и передачи больших объемов информации, увеличивают степень свободы потребления информационных продуктов. Так, эфирное телевидение

построено на традиционном подходе к исчислению времени, привязывающем зрителя к сетке вещания. Тогда как видеохостинги (YouTube, Vimeo и пр.) и видеоконтентные проекты социальных сетей позволяют потребять информацию в любое время по запросу пользователя. Печатные СМИ с относительно невысокой степенью воспроизводимости проигрывают контенту интернет-проектов, позволяющих организовать гораздо более удобный доступ к информации.

Отсталость регулирования, основанного на традиционной линейной хронологии, хорошо прослеживается в публично-правовой сфере. Например, традиционные представления об исчислимости времени лежат в основе правил определения агитационного периода на выборах. Статьей 49 Федерального закона «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» от 12 июня 2002 г. № 67-ФЗ[13] установлено, что предвыборная агитация на каналах организаций телерадиовещания, в периодических печатных изданиях и в сетевых изданиях проводится в период, который начинается за 28 дней до дня голосования и прекращается в ноль часов по местному времени дня, предшествующего дню голосования, а в случае принятия решения о голосовании в течение нескольких дней подряд – в ноль часов по местному времени первого дня голосования. Проведение предвыборной агитации, агитации по вопросам референдума в день голосования запрещается.

Однако в статье 49 Федерального закона «Об основных гарантиях…» не говорится о наиболее актуальных сегодня средствах распространения информации о выборах – видеохостингах, социальных сетях и мобильных приложениях. Они не имеют правового ста-

[13] Собрание законодательства РФ. – 2002. – 17 июня. – № 24. – Ст. 2253.

туса организаций телерадиовещания, периодических печатных изданий, сетевых изданий. Но при этом оказывают на аудиторию влияние, сопоставимое с ними, а в ряде случаев и превосходящее их.

Новые медиа пребывают в «серой зоне», не в полной мере охваченной правовым регулированием. Это позволяет им доставлять агитационные сообщения в любое время неограниченному кругу лиц. Механизм работы видеохостингов таков, что распространение ими агитационных материалов в день голосования формально не образует состав правонарушения. Материалы размещаются в пределах разрешенного агитационного периода, но в результате работы автоматических алгоритмов предлагаются пользователю уже после его окончания – когда агитация запрещена. Налицо проблема, вызванная применением линейной хронологии, к регулированию технологий, свойственных цифровому пространству. На наш взгляд, ее решение может привести к отказу от попыток ограничения распространения информации в зависимости от наступления определенных событий. Не исключено, что «День тишины» и подобные запретительные меры в цифровом мире утратят разумные основания.

При этом на первый взгляд очевидный способ радикального решения проблемы – техническая блокировка новых каналов распространения информации, является заведомо неэффективной. Она игнорирует важнейшую закономерность жизни в информационном обществе – новые способы и каналы распространения информации появляются быстрее, чем оказываются заблокированы старые.

1.6. Тестовые задания

1. Цифровое право в широком смысле – это:
   - новая комплексная отрасль права;
   - межотраслевой правовой институт;
   - новое направление правового регулирования;
   - основная отрасль права.

2. Цифровое право в широком смысле:

- предполагает выделение особого правового института;
- основано на признании особых правовых свойств цифровой информации;
- основано на применении методологии частного права;
- определено в Федеральном законе «Об информации, информационных технологиях и защите информации» как специальный правовой режим цифровой информации.

3. Цифровое право в узком смысле – это:

- основная отрасль российского права;
- совокупность норм государственного права;
- комплексный межотраслевой правовой институт;
- институт гражданского права, содержащий нормы, регулирующие реализацию технологий искусственного интеллекта.

4. Цифровое право как комплексный межотраслевой правовой институт – это:

- вторичное правовое образование, объединяющее нормы, регулирующие отношения, связанные с использованием цифровых данных;
- новая отрасль права;
- системная правовая доктрина информационного общества;
- совокупность норм гражданского права.

5. В каком действующем правовом акте дано легальное определение информации?

- в Конституции Российской Федерации;
- в Федеральном законе «Об информации, информационных технологиях и защите информации»;
- в Федеральном законе «Об информации, информатизации и защите информации»;
- в Гражданском кодексе Российской Федерации.

6. Медиатизация как свойство цифровой информации означает, что:

- она участвует в коммуникации через посредника;
- необходимым элементом отношений с участием цифровой информации является техническая система;
- свойствами медиасреды при регулировании отношений, связанных с цифровой информацией, можно пренебречь;
- коммуникация с использованием цифровых данных регулируется только техническими нормами.

7. Данные в цифровой форме – это:

- информация, представленная в виде дискретных символов;
- сведения о техническом регулировании;
- один из видов информации;
- информация, которая не может быть представлена в виде электронного документа.

8. Согласно Федеральному закону «Об информации, информационных технологиях и защите информации» от 27 июля 2006 г. № 149-ФЗ, информация – это:

- коммуникация;
- данные;
- сведения;
- сообщения;
- факты.

9. В отношении цифровой информации:

- возможно осуществление права собственности;
- невозможно осуществление права распоряжения;
- невозможно осуществление права владения;
- невозможно осуществление права пользования.

10. Свойство неисчерпаемости цифровой информации обеспечивается:

- неподверженностью цифровой информации физическому старению;
- одновременной доступностью цифровой информации с территории разных государств;
- субъективность ее восприятия;
- недоступностью для восприятия человеком без специальных технических средств.

1.7. Список литературы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). – URL: http://www.pravo.gov.ru (дата обращения: 01.02.22).
2. Договор о Евразийском экономическом союзе (подписан в г. Астане 29.05.2014). – URL: http://www.pravo.gov.ru (дата обращения: 01.02.22).
3. Решение Высшего Евразийского экономического совета от 11.10.2017 № 12 «Об Основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года». – URL: http://www.eaeunion.org (дата обращения: 01.02.22).
4. A Declaration for the Future of the Internet. – URL: https://bit.ly/3wgf9DC (дата обращения: 15.05.22).
5. Федеральный закон от 27.07.2006 № 148-ФЗ «Об информации, информационных технологиях и защите информации» // РГ. – 2006. – 29 июля.
6. Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы». – URL: http://www.pravo.gov.ru (дата обращения: 01.02.22).

7. Актуальные проблемы информационного права: учебник / коллектив авторов; под ред. И.Л. Бачило, М.А. Лапина. – М.: Компания КноРус, 2019. – 594 с.

8. Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право: учебник / под ред. акад. Б.Н. Топорнина. – СПб.: Юридический центр Пресс, 2001. – С. 145.

9. Венгеров А.Б. Право и информация в условиях автоматизации управления. – М.: Юрид. лит., 1978.

10. Глушков В.М. О кибернетике как науке. – М.: Наука, 1964. – 53 с.

11. Зорькин В.Д. Право против хаоса. 2-е изд., испр. и доп. – М.: Норма: ИНФРА-М., 2018. – 368 с.

12. Информационное пространство: обеспечение информационной безопасности и права: сб. науч. трудов / под ред. Т.А. Поляковой, В.Б. Наумова, А.В. Минбалеева. – М.: ИГП РАН, 2018. – 512 с.

13. Концепция цифрового государства и цифровой правовой среды: монография / Н.Н. Черногор, Д.А. Пашенцев, М.В. Залоило [и др.]; под общ. ред. Н.Н. Черногора, Д.А. Пашенцева. – М.: Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации; Норма: ИНФРА-М, 2021.

14. Кузнецов П.У. Правовая методология информационных процессов и информационной безопасности (вербальный подход). – Екатеринбург, 2001. – 171 с.

15. Моль А. Теория информации и эстетическое восприятие. – М.: Мир, 1966. – С. 15.

16. Основы цифровой экономики: учебное пособие / коллектив авторов; под ред. М.И. Столбова, Е.А. Бренделевой. – М.: ИД «Научная библиотека», 2018. – 238 с.

17. Правовое регулирование цифровой экономики в современных условиях развития высокотехнологичного бизнеса в национальном и глобальном контексте: монография / Под общ. ред. В.Н. Синюкова, М.А. Егоровой. – М.: Проспект, 2019. – 240 с.

18. Степин В.С. Теоретическое знание. – М.: Прогресс-Традиция, 1999. – 392 с.

19. Терещенко Л.К. Правовой режим информации. – М.: Юриспруденция, 2007. – 192 с.

20. Юридическая концепция роботизации: монография / отв. ред. Ю.А. Тихомиров, С.Б. Нанба. – М.: Проспект, 2019. – 240 с.

21. Урсул А.Д. Информация. – М.: Наука, 1971. – 296 с.

22. Цифровая экономика: проблемы правового регулирования: монография / В.В. Зайцев, О.А. Серова [и др.]. – М.: Кнорус, 2019. – 200 с.

23. Цифровизация правотворчества: поиск новых решений: монография / Д.А. Пашенцев, М.В. Залоило, О.А. Иванюк, А.А. Головина; под общ. ред. д-ра юрид. наук, проф. Д.А. Пашенцева. – М.: Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации: ИНФРА-М, 2019.

ГЛАВА II. СОЦИАЛЬНЫЕ ОСНОВАНИЯ ПРАВОВОГО РЕГУЛИРОВАНИЯ ЦИФРОВЫХ ОТНОШЕНИЙ

2.1. Потребительская культура информационного общества

Содержание позитивного права определяется экономическими отношениями, поэтому важно понимать, что информационное общество – это не только пространства добра и справедливости, но и общество потребительской культуры, прямо или косвенно обслуживающей рынки материальных и символических ценностей[14]. Цифровые данные легко копируются и распространяются, что делает возможным их массовое производство и потребление. Кроме того, применение информационных технологий, в отличие от аналоговых, обеспечивает высокий уровень прибавочной стоимости. Превращение цифровой информации в товар означает распространение на нее закономерностей спроса и предложения. При этом неисчерпаемость и нематериальность цифровой информации приводят к проявлению на цифровых рынках уникальных экономических эффектов, которые должны учитываться в правовом регулировании.

Наиболее интересным с точки зрения реализации правовых норм является так называемый эффект Стрейзанд. Он важен для понимания пределов возможностей права в ограничении нежелательной для государства информации. Эффект Стрейзанд, назван по имени американской актрисы Барбары Стрейзанд, предпринимавшей настолько серьезные меры по охране своей частной жизни, что это вызывало повышенное внимание со стороны общества, которое в итоге оказалось сильнее юридических норм. Особенности частной жизни, которые она охраняла от вмешательства журналистов стали

[14] См. Долгин А. Экономика символического обмена. – М.: Инфра-М, 2006. – 632 с.

общеизвестны во многом не вопреки, а благодаря экстраординарным мерам, которые были предприняты для обеспечения конфиденциальности информации.

Эффект Стрейзанд – социально-экономический феномен, заключающийся в существенном увеличении спроса на информацию, которая подвергается ограничению. Он распространяется на любую информацию независимо от ее цифровой или аналоговой природы, но с наибольшим эффектом проявляется именно в отношении цифровых данных. Их легко скопировать, перенести их источник в другую юрисдикцию или другим способом обеспечить удовлетворение повышенного спроса на информацию.

Анализ дел судебной и административной практики в России убедительно свидетельствует о проявлении эффекта Стрейзанд и непродуктивности правовых решений, не учитывающих его. Достаточно упомянуть два эпизода новейшей цифровой истории России – попытку блокировки страницы Википедии с информацией о наркотическом веществе чарас на основании Решения Черноярского районного суда Астраханской области от 25 июня 2015 г. и неудачное ограничение доступа к информационным ресурсам Telegram Messenger LLP по решению Таганского районного суда г. Москвы от 13 апреля 2018 г. № 2-1779/2018. В обоих случаях непродуманные меры по ограничению доступа к цифровой информации стимулировали рост спроса на нее, который был удовлетворен. Популярность статьи в Википедии, которая вопреки решению суда так и не была заблокирована, выросла в 1000 раз, пиковое значение ее аудитории достигало более 100 000 пользователей в сутки[15]. Эффект Стрейзанд оказался сильнее эффекта права. Воля суда не просто

[15] В 1000 раз выросла популярность запрещённой вики-статьи про наркотик, после того как Роскомнадзор публично «саботировал» блокировку материала. – URL:.https://bit.ly/32z9sER (дата обращения: 01.02.2022).

была проигнорирована. Фактически попытка ограничить доступ к цифровой информации без учета ее особенностей привела массовому распространению информации о наркотиках. Попытка ограничения доступа к Telegram в России также привела к обратному эффекту – росту российской ежедневной аудитории приложения на 31%[16].

2.2. Научно-технический прогресс как ценность

Другой важной особенностью информационного общества, имеющая значение для права – понимание научно-технического прогресса как ценности.

Реализация цифровых технологий имеет очевидные позитивные результаты – распространение знаний, освобождение человека от рутины и т.д. Поэтому представление о техническом прогрессе как общественной ценности вполне обосновано. При этом осознание важности цифровых технологий для общества не всегда находит свое выражение в праве. Для примера можно привести известное судебное решение по делу о жалобе А.Л. Буркова на ООО «Гугл» (дело № 2-783/2015 ~ М-8090/2014). Суть претензии сводилась к тому, что истец потребовал прекращения чтения своей электронной переписки на gmail.com роботами Google. Он обнаружил это в связи с тем, что компания предлагала ему контекстную рекламу на основе содержания его писем. Несмотря на то, что факт анализа электронных сообщений роботами бесплатных почтовых сервисов уже тогда был общеизвестен и пользовательское соглашение Gmail содержало явное указание на возможность автоматизированного анализа содержания сообщений, истец счел, что оно не соответствует нормам конституционного права на тайну переписки и

[16] Эксперты зафиксировали рост использования Telegram после блокировки. – URL:. https://bit.ly/3o2p6Qy (дата обращения: 01.02.2022).

не должно применяться. Суд встал на сторону истца, сделав вывод, что Гугл, размещая рекламу в сообщении истца, руководствовался результатами мониторинга его электронной корреспонденции, тем самым нарушил тайну переписки. Суд запретил ООО «Гугл» встраивать рекламу в переписку истца и обязал ответчика компенсировать моральный вред.

На наш взгляд, указанное решение вызывает озабоченность с точки зрения понимания закономерностей развития цифровых технологий. Во-первых, обработка почтовых сообщений роботом происходит без непосредственного изучения человеком и поэтому ее квалификация как нарушение тайны переписки вызывает обоснованные сомнения. Во-вторых, запрет на изучение сообщений электронной почты, а значит и использование их содержания для персонализации рекламных сообщений препятствует реализации бизнес-модели Google, благодаря которой компания получает возможность предоставлять доступ ко многим своим сервисам бесплатно. Очевидно, что исполнение решения суда привело к серьезной перестройке технологических процессов, повлекшей для компании непредвиденные издержки. Вполне вероятно, что в итоге они привели к ухудшению положения потребителей повышению цен на цифровые услуги, оказываемые компаний, или отказу от запуска новых продуктов.

В то же время не менее обосновано суждение о том, что бесконтрольное использование цифровых технологий содержит потенцию к разрушению традиционных ценностей, многие из которых, в отличие от научно-технического прогресса, имеют конституционное признание.

Так, применение технологии распознавания лиц на основе машинного обучения и других вариантов биометрической идентификации может препятствовать полноценной реализации конституци-

онного статуса гражданина. Причем это касается не только конкретных прав и свобод, но и принципов конституционного статуса личности. Для примера, оценим эффект от внедрения биометрии на реализацию конституционного принципа равноправия. На первый взгляд, отношения, связанные с внедрением биометрии, подчеркнуто равноправны. Граждане как правило участвуют в формировании Единой биометрической системы добровольно, органы государственной власти и крупные коммерческие организации лишены возможности применения публично-властного принуждения. Однако формальное равноправие может быть гарантией равных возможностей только в сфере реализации личных и политических прав. А в экономических отношениях формальное равноправие граждан и крупных организаций всегда оборачивается фактическим неравенством. Гражданин получает формально равные права с субъектом, многократно превосходящим его по материальным, организационным и всем прочим возможностям, а отказ от взаимодействия с ним будет означать необоснованные затруднения в повседневной жизни.

Внедрение биометрической идентификации лишь усугубит фактическое неравенство – любая потенциально конфликтная ситуация будет означать столкновение раз и навсегда идентифицированного гражданина с анонимизированными представителями корпорации, выполняющими прежде всего корпоративные инструкции. Поэтому неизбежное внедрение биометрических технологий в сферу реализации прав личности должно сопровождаться мерами, направленными на защиту гражданина как слабой стороны, имеющей гораздо меньше реальных возможностей, чем ее контрагенты. Во-первых, гражданин должен получить юридические гарантии того, что отказ от представления биометрических данных не приведет к ухудшению его положения по сравнению с другими потреби-

телями коммерческих и государственных услуг. Во-вторых принципиальное значение имеет правило взаимной идентификации – если гражданин идентифицировал себя во взаимоотношениях с корпоративным субъектом, он должен иметь право и реальную возможность получить достоверную информацию о лице, действующем от имени корпорации.

Многие конституционные ценности, связанные с реализацией личных и политических прав, оказываются под более серьезной угрозой. Дополнительные риски возникают в отношении защиты ценностей частной жизни. Развитие технологий идентификации человека по его изображению в сочетании с повсеместным распространением видеонаблюдения существенно ограничивают сферу частной жизни, по сути, ограничивая ее пространством жилища. Это не согласуется с общепринятым в обществе понятием «частная жизнь».

Высказанные предложения носят перспективный характер. Универсальные юридические правила разрешения конфликтов между «цифровыми» и «аналоговыми» ценностями пока не выработаны, а применяемые государством решения носят несистемный характер. В сложившейся ситуации задачу обеспечения баланса ценностей решают не государства, а частные компании. И эти решения не всегда принимаются в пользу новых цифровых технологий. 4 ноября 2021 года компания Meta Platforms[17], заявила об отключении системы распознавания лиц в своей социальной сети и обязалась удалить связанные с ней данные пользователей. Пользователи больше не будут автоматически распознаваться на фотографиях и не будут видеть предложение отметить других пользователей[18]. Это

[17] Суд признал экстремистской и запретил в России деятельность корпорации Meta по реализации социальных сетей Facebook и Instagram.

[18] Facebook Plans to Shut Down Its Facial Recognition System. The New York Times. – URL: https://nyti.ms/3fWwB7t (дата обращения: 01.02.2022).

сделано в связи с увеличением рисков использования персональных данных без необходимых юридических гарантий. В 2018 году Microsoft, Amazon и IBM приняли решение об отказе от продажи своих технологий распознавания лиц органам охраны правопорядка до тех пор, пока не будут приняты правовые акты, определяющие пределы ее разрешенного использования[19].

Частные компании и общественные институты также впереди в деле формирования моральных оснований, на которых должно строиться новое право. Заслуживает внимания инициатива Массачусетского технологического института по исследованию настроений в обществе по поводу вреда, который может быть причинен беспилотными транспортными средствами. – The Moral Machine[20].

2.3. Публичные и частные функции в информационном обществе

Потребительская культура информационного общества существенно изменила представление о разграничении функций публичной власти, частных компаний и общественных институтов. Частные технологические компании сейчас фактически осуществляют полномочия, которые ранее находились в исключительной компетенции органов государства. Деятельность крупнейших корпораций, таких как Alphabet, Apple, Amazon, уже вышла за пределы частных отношений. Они не просто поставщики информационных услуг, а полноценные участники публичной политики, обладающие большим влиянием на общество и принимающие фактически власт-

[19] Microsoft bans police from using its facial-recognition technology. The Washington Post. – URL: https://wapo.st/34f7QRm (дата обращения: 01.02.2022).

[20] Moral Machine. – URL: https://www.moralmachine.net/hl/ru (дата обращения: 01.02.2022).

ные решения. Twitter, Snapchat, Telegram и другие социальные сервисы сегодня имеют возможность исключить из цифрового информационного пространства любое лицо, как это произошло в 2020 году с Президентом США. В России аналогичные социальные функции осуществляет vk.com. ООО «Яндекс» выполняет функции администратора платформы для государственного информирования населения о распространении коронавирусной инфекции. Перечень функций, приватизированных ИТ-компаниями можно продолжать долго.

Обычно цифровая власть технологических компаний рассматривается как их фактическая возможность разрешать или запрещать распространение информации. Наибольший интерес представляют случаи, когда частные компании предпринимают меры, ограничивающие общественно-значимую информацию и фактически имеющие признаки цензуры. Так, последняя редакция политики YouTube в отношении контента запрещает распространение определенной информации о выборах. На платформе не должны распространяться ложные утверждения о том, что массовые избирательные правонарушения, ошибки или сбои повлияли на результат избирательных кампаний после того, как окончательные результаты выборов были официально установлены. В настоящее время это относится к любым состоявшимся президентским выборы в США и Федеральным выборам в Германии 2021 года[21]. Другие выборы почему-то из сферы внимания YouTube выпали. При этом какая-либо формальная процедура определения истинности или ложности утверждений не предусмотрена. Фактически такая деятельность имеет признаки, сходные с политической цензурой.

Публичная деятельность частных компаний отличается от аналогичной деятельности государственных органов. Государственные

[21] Elections misinformation policies – YouTube Help. – URL: https://bit.ly/3AArGmb (дата обращения: 01.02.2022).

органы связаны публичным интересом, имеющим конкретные юридические формы выражения в демократических институтах. Таких как выборы, референдум, публичные акции, обращения граждан. Частные ИТ-компании являются прежде всего коммерческими предприятиями и руководствуются соображениями извлечения прибыли. К ним неприменимы правовые механизмы, обеспечивающие реализацию прав человека и гражданина:

- сменяемость руководства;
- гарантии участия граждан в осуществлении публичных функций;
- гарантии социально-экономических прав, в частности, прав потребителей;
- гарантии защиты прав с помощью судебных и административных процедур.

Для частных компаний также характерен приоритет внутренних правил над нормами национального (в частности, российского) права. Он ярко проявился в уже упомянутом деле о блокировке страницы российской Википедии о наркотическом веществе. Сообщество редакторов Википедии обосновало отказ от удаления информации тем, что эта информация соответствует правилам Википедии[22]. При этом аргумент о необходимости исполнения решения российского суда фактически не был принят во внимание.

Цифровая коммуникация имеет большое значение для реализации важнейших прав – на участие в выборах (электронное голосование), образование, распоряжение способностями к труду, охрану здоровья и медицинскую помощь и др. Например, реализация прав на охрану здоровья и медицинскую помощь невозможна без исчер-

[22] «Википедия» отказалась удалять статью по требованию Роскомнадзора. – URL: https://bit.ly/3Iz8RCk (дата обращения: 01.02.2022).

пывающей информации о системе медицинских учреждений, конкретных специалистах, факторах, создающих угрозу жизни и здоровью населения (ст. ст. 7, 41 Конституции РФ)[23].

В условиях пандемии зависимость прав и свобод от цифровой формы их реализации стала очевидной. Для полноценной реализации своего правового статуса гражданин вынужден вступать в правоотношения с частными компаниями – основными участниками рынка цифровых продуктов. Как правило это происходит в форме договора присоединения, на условия которого гражданин не имеет возможности повлиять. Установлено, что человек не только не склонен читать пользовательские соглашения с поставщиками цифровых сервисов, но и объективно не может этого сделать. В результате исследования, проведенного в университете Карнеги Меллон оказалось, что каждый пользователь сети для принятия осознанного информированного решения о присоединении к соглашению на каждом сайте, которым он пользуется, должен провести 25 дней в году круглосуточно изучая тексты соглашений. Если уделять этому 8 часов в день, потребуется 76 дней[24]. Гражданин обычно не имеет необходимых ресурсов чтобы осознать условия, которые ему предлагается принять.

Личность попадает в зависимость к своему контрагенту и становится слабой стороной договорных отношений. Это обеспечивает сильной стороне возможность администрирования. Крупнейшие участники информационного рынка приобретают управленческие полномочия и соответствующие публичные функции. Справедливым будет распространение на них и обязанностей, характерных

---

[23] Тарасенкова А.Н. Информационное право: возрастная маркировка, цифровая безопасность и другие вопросы. М.: Редакция «Российской газеты». 2019. – Вып. 20. – 176 с.

[24] You'd Need 76 Work Days to Read All Your Privacy Policies Each Year // techland.time.com. – URL: https://bit.ly/3u0qsza (дата обращения: 01.02.2022).

для публичной власти. В частности, оправданным представляется возложение на субъектов специализированной информационной деятельности обязанности рассматривать обращения граждан и их объединений в порядке, предусмотренном Федеральным законом «О порядке рассмотрения обращений граждан Российской Федерации». Отчасти данное предложение реализовано в Федеральном законе «О деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации» от 1 июля 2021 г. № 236-ФЗ.

2.4. Равенство и равноправие в условиях сетевой инфраструктуры цифровой информации

Современные информационные сети функционируют по закону предпочтительного присоединения. Его эффект состоит в том, что ценности равноправия и социальной справедливости в сетевых отношениях проявляются в меньшей степени, чем в обычной жизни.

Закон предпочтительного присоединения объясняется так: когда в сети появляется новый узел, вероятность его связи с любым другим узлом, уже включенным в сеть, пропорциональна количеству связей, имеющихся у этого узла[25]. Другими словами, узлы с большим числом связей получают еще больше связей. Известные становятся еще известнее. У узла с наибольшим количеством связей самые высокие шансы на получение новых, и чем больше их у него появляется, тем привлекательнее он становится. Популярность в сети определяется количеством ссылок. Популярность привлекательна и поэтому тому, у кого что-то есть, дается еще больше. Новые пользователи социальной сети с большой долей вероятности

[25] Albert-László Barabási, Jennifer Frangos. Linked: How Everything Is Connected to Everything Else and What It Means for Business, Science, and Everyday Life. Hachette UK, 2014.

будут подписываться на аккаунты пользователей, которые уже имеют большое число подписчиков, тем самым способствуя росту их популярности[26].

Если упорядочить узлы по числу связей и построить график, получится кривая обратно-пропорциональной зависимости с длинным хвостом. В хвосте оказывается абсолютное большинство узлов – пользователей со сравнительно небольшим числом связей. Напротив, хабы – наиболее известные узлы с миллионами связей немногочисленны, их буквально считанные единицы.

Исследователи видят в этом проявление правила Парето, выражающего обратно-пропорциональную зависимость. Закон Парето был выявлен при измерении благосостояния населения стран в начале XX века и означал, что в руках небольшой группы наиболее преуспевающих людей (не более 20%) сосредоточена основная часть капитала (до 80%). С тех пор была подтверждена применимость этого правила к объяснению многих аспектов общественной жизни. В том числе к объяснению закономерностей развития информационных сетей.

Обратно-пропорциональной зависимости подчиняется популярность сайтов, объем передаваемых в сети файлов, рейтинг пользователей социальных сетей по числу подписчиков. Важно понимать, что соотношение 20% к 80% математически является приблизительным. В то же оно позволяет преодолеть так называемое заблуждение 50/50 – иллюзии об одинаковом значении разных факторов, которая на первый взгляд представляется логичной и является социальным основанием для правового равенства. Таким образом, сетевая структура цифровых данных способствует монополизации

[26] См. Больц, Н. Размышление о неравенстве. Анти-Руссо / пер. с нем. И. А. Женина; под науч. ред. Я. Н. Охонько; Нац. исслед. ун-т «Высшая школа экономики». – М.: Изд. дом Высшей школы экономики, 2014.

оборота цифровой информации и требует специальных мер, направленных на поддержку конкуренции.

Эффективность регулирования цифровых отношений также зависит от учета упомянутого принципа. В частности, непрактичны запреты и ограничения, игнорирующие особенности сетевой структуры. Закон предпочтительного присоединения подсказывает, что прежде всего необходимо ограничивать нежелательную информацию, исходящую от крупных хабов социальных сетей. То есть от пользователей с сотнями тысяч и миллионами связей. Однако правоприменительная практика складывается иначе – чаще всего к ответственности за распространение, например, экстремистских материалов привлекаются пользователи имеющие единицы и десятки подписчиков в социальных сетях. Показательным в этом отношении является дело Александра Бубеева[27], осужденного на 2 года и 3 месяца лишения свободы за публичные призывы к экстремистской деятельности и нарушению территориальной целостности Российской Федерации. Публичность его призывов выразилась в их распространении среди двенадцати подписчиков в социальной сети «Вконтакте». Формальные основания для привлечения к ответственности безусловно были, но вряд ли можно согласиться с тем, что уголовное наказание достигло всех своих целей. Инициировав уголовное преследование, правоохранительные органы поместили в центр общественного внимания информацию, которая с очень высокой долей вероятности никогда бы туда не попала. Таким образом они стимулировали проявление эффекта Стрейзанд. Общественная кампания в защиту обвиняемого сделала его и его взгляды широко известными. Поиск Google дает доступ к четырнадцати тысячам страниц, на которых упоминается его дело и к трем тысячам страницам с упоминанием спорной статьи, за распространение которой

[27] URL: https://bit.ly/32BTAl8 (дата обращения: 01.02.2022).

он был наказан. Эти величины несопоставимы с исходной аудиторией в 12 подписчиков.

2.5. Тестовые задания

При выполнении тестовых заданий необходимо выбрать из представленных ответов на вопрос один или несколько вариантов.

1. Какие свойства цифровой информации способствуют проявлению уникальных экономических эффектов?

- неисчерпаемость;
- нематериальность (идеальность);
- аналоговая форма;
- недоступность для восприятия человеком.

2. Эффект Стрейзанд заключается:

- в болезненном пристрастии к творчеству Барбары Стрейзанд;
- в существенном увеличении спроса на цифровую информацию, доступ к которой подвергается ограничению;
- в существенном снижении интереса к информации, доступ к которой подвергается ограничению.

3. Проявление эффекта Стрейзанд усматривается в последствиях:

- ограничения доступа к информационным ресурсам Telegram Messenger LLP по решению Таганского районного суда г. Москвы от 13 апреля 2018 г. № 2-1779/2018;
- запрета на автоматический мониторинг сообщений электронной почты на основании Апелляционного определения по жалобе А.Л. Буркова на решение Замоскворецкого районного суда г. Москвы от 21 апреля 2015 года (дело № № 33-30344);

- реализации права на поиск и получение информации о деятельности государственных органов и органов местного самоуправления;

- исполнения Решения Черноярского районного суда Астраханской области от 25 июня 2015 г. о признании информации, размещенной в Википедии, запрещенной на территории Российской Федерации.

4. Автоматический мониторинг содержания электронных сообщений граждан Российской Федерации, передаваемых с помощью общедоступных сервисов электронной почты:

- признается нарушением конституционного права на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений;

- не признается нарушением конституционного права на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений при условии, если мониторинг сообщений производится без участия человека;

- не признается нарушением конституционного права на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений при условии, если владельцем сервиса электронной почты является юридическое лицо с местом нахождения в Российской Федерации;

- не признается нарушением конституционного права на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений при условии, если владельцем сервиса электронной почты является юридическое лицо с местом нахождения в стране Евразийского экономического союза.

5. Внедрение технологий биометрической идентификация человека:

- содержит потенциальную угрозу реализации конституционного права на неприкосновенность частной жизни;

- способствует усилению юридических гарантий конституционного права на неприкосновенность частной жизни;

- требует реализации юридических мер для защиты прав и свобод гражданина как слабой стороны экономических отношений.

6. ИТ-компании как коммерческие организации:

- осуществляют деятельность на основе приоритета их внутренних правил над нормами национального права;

- связаны публичным интересом, имеющим конкретные юридические формы выражения в демократических институтах;

- применяют принципы всеобщего, равного и прямого избирательного права для замещения должностей в их руководящих органах;

- предусматривают гарантии прав граждан на участие в управлении их деятельностью.

7. Крупнейшие ИТ-компании:

- являются коммерческими организациями;

- фактически осуществляют публичные функции;

- являются публично-правовыми образованиями;

- имеют статус международных организаций.

8. Закон предпочтительного присоединения узлов в сети:

- способствует равноправию в отношениях, связанных с распространением цифровой информации;

- препятствует реализации ценностей равноправия и социальной справедливости;

- способствует монополизации отношений, связанных с обработкой цифровых данных;

- способствует распространению идеологии коллективизма.

9. Закон предпочтительного присоединения означает, что:

- у узла с наибольшим количеством связей самые высокие шансы на получение новых связей;

- у узла с наибольшим количеством связей самые низкие шансы на получение новых связей;

- у узла с наименьшим количеством связей самые высокие шансы на получение новых связей.

10. Действующая политика YouTube в отношении контента:

- запрещает распространение ложных утверждений о том, что массовые избирательные правонарушения, ошибки или сбои повлияли на результаты выборов Президента Российской Федерации 2018 года;

- запрещает распространение ложных утверждений о том, что массовые избирательные правонарушения, ошибки или сбои повлияли на результаты выборов Президента США 2000 года;

- запрещает распространение ложных утверждений о том, что массовые избирательные правонарушения, ошибки или сбои повлияли на результаты федеральных выборов в ФРГ 2021 года;

запрещает распространение информации о том, что массовые избирательные правонарушения, ошибки или сбои повлияли на результат любых состоявшихся выборов.

2.6. Список литературы

1. Белов В.А. Общая часть. Т. II: Лица, блага, факты: учебник. – М.: Юрайт, 2011. – 463 с.

2. Больц Н. Размышление о неравенстве. Анти-Руссо / пер. с нем. И.А. Женина; под науч. ред. Я.Н. Охонько. – М.: Изд. дом Высшей школы экономики, 2014.

3. Винья П., Кейси М. Эпоха криптовалют: как биткоин и блокчейн меняют мировой экономический порядок / пер. с англ.

Э. Кондуковой; науч. ред. А. Форк. – М.: Манн, Иванов и Фербер, 2017.

4. Генкин А., Михеев А. Блокчейн: как это работает и что ждет нас завтра. – М.: Альпина Паблишер, 2018. – 592 с.

5. Институты и путь к современной экономике. Уроки средневековой торговли / пер. с англ. И. Кушнаревой. – М.: Изд. дом Высшей школы экономики, 2013.

6. Лапидус Л.В. Цифровая экономика: управление электронным бизнесом и электронной коммерцией: монография. – М.: ИНФРА-М, 2018. – 381 с.

7. Морхат П.М. Искусственный интеллект. Правовой взгляд. – М., 2017.

8. Нагродская В.Б. Новые технологии (блокчейн / искусственный интеллект) на службе права: научно-методическое пособие / Под ред. Л.А. Новоселовой. – М.: Проспект, 2019. – 128 с.

9. Новые законы робототехники. Регуляторный ландшафт. Мировой опыт регулирования робототехники и технологий искусственного интеллекта / [В. Бакуменко и др.]; под ред. А.В. Незнамова. – М.: Инфотропик Медиа, 2018.

10. Основы государственной политики в сфере робототехники и технологий искусственного интеллекта / [А. Бутримович и др.]; под ред. А.В. Незнамова. – М.: Инфотропик Медиа, 2019. – 184 с.

11. Правовое регулирование экономических отношений в современных условиях развития цифровой экономики: монография / А.В. Белицкая, В.С. Белых, О.А. Беляева [и др.]; отв. ред. В.А. Вайпан, М.А. Егорова. – М.: Юстицинформ, 2019.

12. Правовое регулирование цифровой экономики в современных условиях развития высокотехнологичного бизнеса в национальном и глобальном контексте: коллективная монография / Под общ. ред. В.Н. Синюкова, М.А. Егоровой. – М.: Проспект, 2019.

13. Регулирование робототехники: введение в «робоправо». Правовые аспекты развития робототехники и технологий искусственного интеллекта / [В.В. Архипов и др.]; под ред. А.В. Незнамова. – М.: Инфотропик Медиа, 2018. – 232 с.

14. Самолысов П.В. Информатизация образования. Избранные научные труды: монография. – М.: АИО, 2011. – 188 с.

15. Сырых В.М. Теория государства и права: учебник. – М.: Юстицинформ, 2012.

16. Тарасенкова А.Н. Информационное право: возрастная маркировка, цифровая безопасность и другие вопросы. – М.: Редакция «Российской газеты». 2019.

17. Цифровой бизнес: учебник / под науч. ред. О.В. Китовой. – М.: ИНФРА-М, 2018.

18. Шарма Р. Взлеты и падения государств. Силы перемен в посткризисном мире / пер. с англ. Н. Шаховой. – М.: АСТ; CORPUS, 2018.

19. Шваб К., Дэвис Н. Технологии Четвертой промышленной революции / пер. с англ. – М.: Эксмо, 2018.

20. Цифровая трансформация и государственное управление: научно-практическое пособие / А.С. Емельянов, А.А. Ефремов, А.В. Калмыкова [и др.]; ред. кол.: Л.К. Терещенко, А.С. Емельянов, Н.А. Поветкина. – М.: Инфотропик Медиа, 2022.

21. Цифровая экономика: актуальные направления правового регулирования: научно-практическое пособие / под ред. И.И. Кучерова, С.А. Синицына. – М.: Норма: ИЗиСП, 2022.

22. Albert-László Barabási, Jennifer Frangos. Linked: How Everything Is Connected to Everything Else and What It Means for Business, Science, and Everyday Life. Hachette UK, 2014.

ГЛАВА 3. СУБЪЕКТЫ ЦИФРОВЫХ ПРАВООТНОШЕНИЙ

3.1. Обладатель цифровой информации

Цифровые данные – это информация. Поэтому определение участников цифровых правоотношений следует начать с положений акта, обладающего высшей юридической силой в системе источников информационного права – с Конституции Российской Федерации.

Различным аспектам информационных отношений в Конституции посвящена далеко не одна статья (см. ст. 23, 29, 33, 44, п. «и» статьи 71), при этом определяющее значение для статуса носителей цифровых прав являются положения части 4 статьи 29. Согласно ему каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Содержание информационных возможностей будет описано в четвертом модуле. А пока в приведенной формулировке нас может заинтересовать использование характеристики «каждый» применительно к лицу, которое обладает цифровыми права.

По смыслу Конституции, «каждый» – это не только физическое лицо – человек, выступающий в статусе гражданина, иностранного гражданина или лица без гражданства, это и коллективы – Российская Федерация, субъекты Российской Федерации, муниципальные образования, юридические лица[28]. Очевидно, что при формальном равенстве возможностей индивидуальные и коллективные субъекты осуществляют их по-разному. Закон об информации обеспечи-

[28] Постановление Конституционного Суда РФ от 18.07.2012 № 19-П «По делу о проверке конституционности части 1 статьи 1, части 1 статьи 2 и статьи 3 Федерального закона «О порядке рассмотрения обращений граждан Российской Федерации» в связи с запросом Законодательного Собрания Ростовской области» // Собрание законодательства РФ. – 2012. – 30 июля. – № 31. – Ст. 4470.

вает единый подход к определению правовых возможностей субъектов, различных по своей природе и фактическим возможностям. Он реализован в законе в статусе обладателя информации. Согласно закону обладатель информации – это лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации.

Перечень прав обладателя информации открыт, он допускает широкое толкование. Важнейшие из них – разрешать или ограничивать доступ к информации, использовать информацию, в том числе распространять ее, передавать информацию другим лицам, защищать ее от незаконного доступа других лиц.

Большой объем прав обладателя информации согласуется с целью, которую преследовал законодатель вводя это понятие. Она состоит в описании статуса лица, правомочного решать вопрос о получении конкретной информации другими лицами. Прослеживается очевидная аналогия с гражданско-правовыми категориями «собственник» или «титульный владелец», но с учетом особенностей информации как нематериального объекта[29]. Как уже отмечалось, особенность информации состоит в ее нематериальной природе, а то, что нематериально, не может быть физически утрачено. Поэтому владеть информацией физически невозможно, что также означает невозможность распространения на нее системы прав собственника по российскому гражданскому праву. Сказанное позволяет описать обладателя информации как субъекта, осуществляющего наибольший объем информационных прав и обязанностей в отношении цифрового объекта.

---

[29] См. Постановление Конституционного Суда РФ от 26.10.2017 № 25-П «По делу о проверке конституционности пункта 5 статьи 2 Федерального закона «Об информации, информационных технологиях и о защите информации» в связи с жалобой гражданина А.И. Сушкова» // Собрание законодательства РФ. – 2017. – 6 ноября. – № 45. – Ст. 6735.

Как быть в случае, когда доступ к одной и той же информации имеют многие? Означает ли наличие у конкретного лица фактического доступа к информации, что это лицо признается ее обладателем и вправе совершать в отношении нее всю полноту информационных прав? Например, использовать или передавать другим лицам? В особенности это касается цифровой информации, которая обычно используется как элемент информационной системы. Например, доступ к сообщению, переданному с помощью общедоступного сервиса электронной почты есть не только у отправителя и получателя, но и у оператор почтового сервиса. Практика Конституционного Суда РФ дает отрицательный ответ – оператор информационной системы не вправе самостоятельно разрешать или ограничивать доступ к информации, которая передается с его участием. Причем он не может получить такое право даже если оно будет передано в соответствии с пользовательским соглашением. Обязанность обрабатывать и хранить информацию не предполагает право разрешать или ограничивать доступ к этой информации, принадлежащее ее обладателю, которым в данном случае выступает отправитель электронного сообщения.

3.2. Информационный посредник

Обработка цифровых данных возможна только с помощью специальной технической инфраструктуры. Ее функционирование обеспечивают специальные субъекты информационных отношений. В доведении информации до всеобщего сведения через сеть Интернет, как правило, участвуют провайдер доступа к сети, администратор домена, владелец сайта, провайдер хостинга, регистратор доменов, лицо, оператор поисковой системы и другие участники цифровой инфраструктуры.

Они предоставляют обладателям и пользователям информации техническую возможность доступа к ней. Их деятельность является

условием реализации информационных прав другими лицами. В то же время они могут обеспечивать и незаконный оборот цифровых данных, что требует определения степени ответственности информационных посредников. Привлечение их к ответственности за деятельность лиц, передающих и получающих информацию, было бы чрезмерным. Фактически они несли бы ответственность за действия других лиц без собственной вины.

В Российской Федерации универсального регулирования статуса информационных посредников пока нет. Понятие «информационный посредник» определено в статье 1253.1 Гражданского кодекса РФ лишь для целей установления особенностей ответственности за нарушение интеллектуальных прав. К информационным посредникам отнесены лица:

- осуществляющие передачу материала в интернет (провайдеры доступа к сети);
- предоставляющие возможность размещения материала или информации (например, провайдеры хостинга и владельцы сайтов);
- предоставляющие доступ к материалу в этой сети (например, администраторы поисковых систем).

Информационный посредник, осуществляющий передачу материала (провайдер доступа) освобождается от ответственности за нарушение интеллектуальных прав если:

1) он не является инициатором этой передачи и не определяет получателя указанного материала;

2) он не изменяет материал;

3) он не знал и не должен был знать о том, что использование информации является неправомерным. Например, сайт-файлообменник, только хранит и передает информацию, загруженную на него пользователями. Если пользователь загрузит на него файл с контрафактным материалом, файлообменник, признанный информационным посредником, будет освобожден от ответственности.

Информационный посредник, предоставляющий возможность размещения материала в информационно-телекоммуникационной сети, не несет ответственность если:

1) он не знал и не должен был знать о том, что использование информации является неправомерным;

2) он в случае получения в письменной форме заявления правообладателя своевременно принял необходимые и достаточные меры для прекращения нарушения интеллектуальных прав.

Например, признанный информационным посредником онлайн-маркетплейс может быть освобожден от ответственности за размещение на нем информации о продаже контрафактных товаров.

Также существуют специальные правила определения лица, ответственного за нарушения законодательства об интеллектуальной собственности, совершенные на сайте в сети Интернет. По общему правилу ответчиком по иску о прекращении использования спорных объектов на сайте является владелец сайта, поскольку именно он самостоятельно определяет порядок использования сайта. Поэтому бремя доказывания того, что спорный материал на сайте размещен третьими лицами, а не владельцем сайта лежит на владельце. При отсутствии таких доказательств считается, что владелец сайта является лицом, непосредственно использующим соответствующие результаты интеллектуальной деятельности или средства индивидуализации.

Владелец сайта устанавливается на основании сведений, размещенных на самом сайте. Согласно ч. 2 ст. 10 Закона об информации владелец сайта обязан размещать на принадлежащем ему сайте информацию о своих наименовании, месте нахождения и адресе, об адресе электронной почты для обеспечения возможности правообладателям направлять претензии по поводу нарушений на сайте. Например, наличие информации о наименовании организации, ее

месте нахождения и адресе, размещение на сайте средств индивидуализации такой организации, ее товаров и услуг может свидетельствовать о том, что данная организация является владельцем сайта.

При этом владельцем сайта также может быть признан администратор доменного имени, которое адресует на соответствующий сайт. В случае участия администратора домена в совершении правонарушения он также может быть привлечен к ответственности. В частности, если он осознанно предоставил возможность использования домена для совершения правонарушений, или в случае получения дохода от неправомерного использования результатов интеллектуальной деятельности или средств индивидуализации. Под администратором домена понимается пользователь, на имя которого зарегистрировано доменное имя.

Завершая рассмотрение вопроса, еще раз подчеркнем разницу в статусах обладателя информации и информационного посредника. Обладатель осуществляет наиболее полный объем информационных прав и обязанностей в отношении цифрового объекта – он вправе разрешать или ограничивать доступ к информации, использовать информацию, в том числе распространять ее, передавать другим лицам, защищать ее от незаконного доступа других лиц. В отличие от обладателя информации, информационным посредником лицо признается, когда оно лишь предоставляет площадку для размещения сайта или информации на сайте и само не имеет отношения к содержанию информации. Меньший объем прав информационного посредника означает и меньшие обязанности – он освобождается от ответственности за нарушение интеллектуальных прав, допущенное с его участием.

3.3. Идентификация и аутентификация субъектов цифровых правоотношений. Простая электронная подпись

Особенностью цифровых правоотношений является сложность определения участвующих в них лиц. Доступ к цифровой информации может происходить, во-первых, на большом расстоянии и, во-вторых, через посредника, которым служит техническая инфраструктура. В результате доступ может быть анонимным. Кроме того невозможность идентификации лица без его согласия рассматривается в цифровом пространстве как ценность. Она лежит в основе многих цифровых технологий, например криптовалют. Операции с криптовалютой проходят без идентификации лиц, сторонам не обязательно иметь достоверные сведения друг о друге. Операции с криптовалютой являются необратимыми, передав криптовалюту, невозможно требовать ее возврата, поэтому идентификация просто избыточна. Также возможно использование технических средств для маскировки пользователя – VPN, прокси-серверов и пр.

При этом право основано на принципе формальной определенности, требующем, чтобы права и обязанности возникали у определенного лица. Это характерно как для публичного, так и для частного права. Например, законодательство о противодействии легализации доходов, полученных преступным путем, обязывает банки проводить банковские операции только с лицами, в отношении которых проведена надлежащая идентификация. Ст. 19 Гражданского кодекса РФ также устанавливает, что гражданин приобретает и осуществляет права и обязанности под своим именем, включающим фамилию и имя, а также отчество, если иное не вытекает из закона или национального обычая. Приобретение прав и обязанностей под именем другого лица не допускается.

Для решения проблем определения субъектов цифровых отношений в Законе о информации предусмотрены понятия идентификации и аутентификации. Идентификация – это мероприятия по

установлению сведений о лице и сопоставлению данных сведений с идентификатором – уникальным обозначением, необходимым для определения такого лица. Аутентификация – проверка лица на принадлежность ему идентификатора и установление правомерности владения им, в результате чего лицо считается установленным.

Важны оба этих процесса: в результате выполнения идентификации выявляется уникальный идентификатор, однозначно определяющий этого субъекта в информационной системе. Например, адрес электронной почты, который выбран пользователем при регистрации в почтовом сервисе. В дальнейшем при необходимости доступа к информации субъект проходит процедуру аутентификации. Например, в форме проверки соответствия введенного пользователем пароля к учётной записи паролю в базе данных почтового сервиса. Если аутентификация успешна, система определяет субъекта в качестве носителя прав и обязанностей.

Важно понимать, что абсолютно надежная идентификация и аутентификация человека в цифровом мире технологически невозможна. Пара логин-пароль может быть скомпрометирована (перехвачена), электронный ключ похищен, изображение радужной оболочки глаза подменено качественной копией. Биометрия также не дает стопроцентного результата. Существует теоретическая вероятность совпадения данных, принадлежащих разным людям. На практике при аутентификации пользователей ограничиваются не абсолютным, а лишь относительным уровнем достоверности доказательства установления личности. Поэтому существует лишь оспоримая юридическая презумпция (предположение) о принадлежности цифровых прав и обязанностей определенному лицу.

Современный уровень развития техники позволяет выделить три типа факторов аутентификации человека. Они могут быть условно обозначены так. Во-первых, «то, что знаю». Таким фактором может быть разделяемый секрет – многоразовые и одноразовые

пароли, правила преобразования информации. Во-вторых, «то, что имею», в данном случае имеются в виду аппаратные аутентификаторы, USB-устройства, смартфоны со специальным приложением. Третий фактор – «то, чем являюсь». Им могут быть биологические и физиологические признаки человека, которые применяются для биометрической идентификации.

Фактор «то, что знаю» лежит в основе такого реквизита электронного документа, как простая электронная подпись. Простой электронной подписью признается цифровая информация, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом. Для ее создания достаточно ввода логинов и паролей или использования кода подтверждения, отправленного в СМС.

Наибольшее распространение имеют простые электронные подписи в виде паролей – сохраняемых в секрете последовательности символов. Они могут быть выбраны самим пользователем, сгенерированы программными или аппаратными средствами, либо назначены администратором информационной системы. Пароли удобны в повседневном использовании, но им присущи очевидные слабости. Они состоят в возможности разгадывания паролей, их перехвате при анализе сетевого трафика выдачи самим пользователем в результате социального инжиниринга. Негативные последствия использования паролей состоят также в возможности блокирования работы системы как реакции на многократный ввод неправильного пароля.

В какой-то мере слабости многоразовых паролей можно устранить путем увеличения числа и вида символов, из которых они составлены. Даже при использовании только символов латинского алфавита время разгадывания пароля из 8 знаков в 3000 раз больше, чем из 6 знаков. Пароль, состоящий из 8 знаков, среди которых есть прописные и строчные буквы, цифры и дополнительные символы,

на компьютере со средними параметрами может быть разгадан лишь за 57 лет непрерывной работы[30].

Например, с помощью простой электронной подписи происходит идентификация лица при получения государственных и муниципальных услуг. Использование этой подписи происходит по правилам информационной системы – системы документооборота на сайте gosuslugi.ru. Оператор информационной системы по запросу пользователя создает и передает ему ключ простой электронной подписи. Ключом является сочетание 2 элементов – идентификатора (логина) и пароля. Идентификатором является СНИЛС заявителя, а паролем ключа – секретная последовательность символов. При этом согласно Федеральному закон «Об организации предоставления государственных и муниципальных услуг» ключи простых электронных подписей для доступа к госуслугам должны предоставляться бесплатно. Пример простой электронной подписи для доступа к государственным и муниципальным услугам показывает возможность их использования в существующей информационной системе.

Возможно использование простой электронной подписи и вне информационной системы. Участники электронного взаимодействия могут заключить соглашение о том, что получение электронного сообщения с определенного адреса электронной почты будет считаться подписанием документа простой электронной подписью. Секретным ключом такой электронной подписи будет пароль к электронному почтовому ящику, ключом проверки электронной подписи – адрес электронной почты. Практика заключения соглашений об использовании простой подписи распространена, например, в сфере потребительского кредитования, когда банк и клиент договариваются об электронном взаимодействии путем заполнения

[30] Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. – Питер, 2019. – С. 786.

электронных форм на сайте банка. Они приобретают статус электронных документов в результате ввода кодов, направленных клиенту посредством СМС-сообщений.

Существенным недостатком простой электронной подписи является то, что с ее помощью можно лишь подтвердить факт формирования электронной подписи определенным лицом. Она не обеспечивает подлинность данных, то есть не гарантирует, что после подписания электронного документа в него не были внесены изменения. В связи с этим сфера применения простой электронной подписи ограничена. Она признается аналогом собственноручной подписи, только если это прямо предусмотрено нормативным правовым актом, нормативным актом Банка России или соглашением лиц, которые собираются обмениваться электронными документами. Например, возможность использования простой электронной подписи для придания электронному документы юридической силы предусмотрена при страховании гражданской ответственности владельцев транспортных средств[31].

Сравнительно низкий уровень защиты информации от искажения при использовании простой электронной подписи объясняет то, что она не может быть использована для аутентификации при направлении документов в налоговые органы, для регистрации юридических лиц и индивидуальных предпринимателей, в суды, для участия в электронных торгах. Также не допускается использование простой электронной подписи для подписания документов, содержащих сведения, составляющие государственную тайну.

---

[31] Указание Банка России от 14.11.2016 № 4190-У (ред. от 15.07.2021) «О требованиях к использованию электронных документов и порядке обмена информацией в электронной форме при осуществлении обязательного страхования гражданской ответственности владельцев транспортных средств».

3.4. Усиленные электронные подписи. Биометрия

Для более надежного определения принадлежности информации используются усиленные электронные подписи. От простой подписи усиленную отличают обязательное наличие:

- закрытого (секретного) ключа электронной подписи (уникальной последовательности символов, предназначенной для создания электронной подписи);
- открытого ключа проверки электронной подписи (уникальной последовательности символов, предназначенной для проверки подлинности электронной подписи);
- сертификата ключа проверки электронной подписи.

Сертификат – электронный документ или документ на бумажном носителе, выданный специальной уполномоченной организацией – удостоверяющим центром. Он подтверждает принадлежность ключа проверки электронной подписи ее владельцу. Удостоверяющий центр выдает подпись только после установления личности обратившегося за ней.

Ключи и сертификат усиленной электронной подписи состоят из длинных последовательностей символов, что практически исключает их запоминание человеком. Как правило, они передаются на материальном носителе, чаще всего на USB-устройстве. Это означает, что усиленные электронной подписи используют фактор аутентификации лица «то, что имею». При применении усиленных электронных подписей участники электронного взаимодействия обязаны обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия. Также они обязаны уведомлять удостоверяющий центр и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении.

В зависимости от степени защищенности выделяют квалифицированные и неквалифицированные электронные подписи. Для неквалифицированной электронной подписи сертификат ключа проверки может не создаваться, либо он может быть создан удостоверяющим центром, не имеющим государственной аккредитации. Поэтому электронный документ, подписанный усиленной неквалифицированной подписью, как и в случае применения простой электронной подписи, имеет юридическую силу, только если это прямо предусмотрено нормативным правовым актом или соглашением сторон. На практике неквалифицированная ЭП используется реже других видов. Например, с ее помощью граждане и некоторые иностранные организации подают электронные документы в налоговый орган через личный кабинет налогоплательщика на сайте ФНС России.

Одним из требований, которым должна соответствовать квалифицированная электронная подпись, является получение квалифицированного сертификата. Он подтверждает, что ключ такой электронной подписи принадлежит его владельцу и выдается только аккредитованным удостоверяющим центром или Минцифры. Перечень аккредитованных удостоверяющих центров доступен на сайте Минцифры России[32].

Информация, подписанная усиленной квалифицированной электронной подписью, в большинстве случаев признается электронным документом юридически равнозначным документу на бумажном носителе с собственноручной подписью и печатью. Такой документ может применяться в любых правоотношениях – при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых

[32] Аккредитация удостоверяющих центров. – URL: https://digital.gov.ru/ru/activity/govservices/2/ (дата обращения: 01.02.2022).

действий. Исключение составляют случаи, когда нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе. Усиленная квалифицированная электронная подпись широко используется для направления документов в органы публичной власти, суды, а также в гражданском обороте.

Фактор аутентификации «то, чем являюсь» используется для наиболее надежной на сегодня аутентификации лица на основе его биометрических показателей. Определение биометрических персональных данных дано в ст. 11 Федерального закона «О персональных данных» – это сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность.

На практике для распознавания могут использоваться как физиологические и биологические данные человека (отпечатки пальцев, 3D-модель лица, код ДНК, ладонь руки, сетчатка глаза, запах, голос), так и поведенческие характеристики (походка, речь), а также их сочетания.

Биометрическая идентификация теоретически возможна и без применения цифровых технологий. Например, начиная с 1970-х годов, Народная полиция Восточной Германии разработала метод распознавания запахов, при котором запахи тела подозреваемых и обвиняемых лиц собирались и сохранялись. Для этого использовались стерильные салфетки, которые герметично хранились в банках. Поскольку технологий оцифровки запахов тогда еще не было, для их распознавания применялись «аналоговые» средства – специально обученные собаки-дифференциаторы[33]. Следы запаха могли быть «либо взяты непосредственно с частей тела подозреваемого,

[33] Kristie Macrakis: Die Stasi-Geheimnisse: Methoden und Technik der DDR-Spionage. Herbig 2009, ISBN 978-3776625929. S. 371ff.

либо конспиративно закреплены на предметах одежды, которые они носили, или на предметах, к которым они прикасались[34]. При этом запахи не использовались в качестве доказательства. В документе Штази говорится, что дифференциация запахов подходит только «для сужения группы подозрительных лиц».

Сегодня в мире применяются в основном пять типов биометрии (модальности): отпечаток пальца, изображение или 3D-модель лица, голос, радужная оболочка глаза и рисунок вен ладони. Особенностью биометрической идентификации на основе цифровых технологий является высокая степень достоверности определения лица и невозможность быстрой смены данных, используемых для аутентификации.

В настоящее время в России по инициативе Министерства связи и массовых коммуникаций, а также Центрального банка создается Единая биометрическая система. Пока в ней размещаются только данные изображения лица человека и данные его голоса. Они используются не по отдельности, а вместе. Идентификация человека и размещение сведений в Единой биометрической системе производится государственными органами и банками при личном присутствии физического лица с его согласия и на безвозмездной основе. Также формирование Единой биометрической системы может производится другими организациями в случаях, определенных законом. Оператором Единой биометрической системы назначено ПАО «Ростелеком».

Оно обеспечивает сбор, обработку, хранение биометрических данных и проверку их соответствия сданным образцам. Важно, что Ростелеком вправе передавать биометрические данные другим лицам. В частности, они передаются коммерческим банкам для удаленной идентификации граждан при оказании банковских услуг.

---

[34] Wörterbuch der Staatssicherheit. GVS JHS 001-400/81, herausgegeben vom BStU. – 1993. – S. 137.

Чувствительность биометрических данных означает необходимость их особой защиты. Ст. 11 Закона о персональных данных предусматривает, что обработка биометрических данных возможна только при условии получения письменного согласия гражданина. Однако п.5 ст. 14.1 Закона об информации допускает, что при формировании Единой биометрической системы оно может быть дано и в форме электронного документа, подписанного простой электронной подписью. Такое согласие признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью данного физического лица[35]. Это существенно упрощает задачу операторов единой биометрической системы, но создает потенциальные риски для граждан.

Во-первых, несмотря на формально добровольный характер регистрации человека в Единой биометрической системе, он может быть фактически принужден к ней. При формальном равноправии, банки обладают несопоставимо большими экономическими возможностями, чем их клиенты. Оператор Единой биометрической системы специально подчеркивает, что граждане, зарегистрированные в ней, получат доступ к лучшим предложениям на рынке[36]. Значит граждане, не сдавшие биометрию могут быть дискриминиро-

[35] Распоряжение Правительства РФ от 30.06.2018 № 1322-р (ред. от 20.10.2021) «Об утверждении формы согласия на обработку персональных данных, необходимых для регистрации гражданина Российской Федерации в единой системе идентификации и аутентификации, и биометрических персональных данных гражданина Российской Федерации в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации» // СЗ РФ. – 2018. – 9 июля. – № 28.

[36] Единая биометрическая система. – URL: https://bio.rt.ru/citizens/ (дата обращения: 01.02.2022).

ваны. С учетом нестабильного имущественного положения значительной части граждан России, краткосрочная выгода от передачи своих биометрических данных может иметь для них решающее значение.

Во-вторых, физиологические, биологические и поведенческие характеристики человека могут использоваться с целями, на которые он не давал согласия. К примеру, информация, переданная банками теоретически может быть использована для определения политических предпочтений гражданина. Результаты исследования, проведенного в 2020 году, показывают, что технология распознавания лиц может эффективно применяться для выявления политической ориентации человека. Обученный алгоритм распознавания лиц правильно определяет политическую ориентацию в 72% случаев. Этот результат значительно лучше случайности (50%), точности определения человеком (55%) или в результате социологического опроса, которая составляет 66%. Точность была одинаковой для разных стран (США, Канада и Великобритания), технологических платформ сред (Facebook, сайты знакомств) и оставалась высокой (69%) независимо от возраста, пола и этнической принадлежности определяемого лица[37].

3.5. Правосубъектность электронных лиц

Внедрение цифровых технологий робототехники создает новую проблематику юридической науки и практики. В жизни людей возникают принципиально новые отношения, участниками которых становятся роботы – носители искусственного интеллекта. Уже сейчас мы можем побеседовать с ботом в чате, поговорить с голосовым помощником по телефону, существуют реализованные технологии

[37] Kosinski M. Facial recognition technology can expose political orientation from naturalistic facial image. Nature.com. – URL: https://www.nature.com/articles/s41598-020-79310-1.pdf (дата обращения: 15.05.2022).

беспилотного транспорта. В то же время общепризнанные этические и правовые требования к искусственному интеллекту еще не выработаны, в этой области существуют лишь экспериментальные решения.

Легальное определение искусственного интеллекта дано в акте, также имеющем экспериментальное значение – Федеральном законе от 24 апреля 2020 г. № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных», определяющем условия для внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве. Согласно закону «искусственный интеллект – это комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека». Эта же формулировка рекомендована Предварительным национальным стандартом РФ ПНСТ 553-2021 «Информационные технологии. Искусственный интеллект. Термины и определения»[38] для использования в нормативных документах, правовой, технической и организационно-распорядительной документации, научной, учебной и справочной литературе.

Интересно, что согласно легальному определению уровень интеллектуальной деятельности человека рассматривается лишь как

[38] Предварительный национальный стандарт Российской Федерации «Информационные технологии. Искусственный интеллект» ПНСТ 553-2021. – URL: https://bit.ly/3g09skg (дата обращения: 01.02.2022).

минимально допустимый для искусственного интеллекта. То есть носитель искусственного интеллекта по замыслу законодателей должен быть более разумным, чем человек. Это позволяет уверенно говорить о том, что участие носителей искусственного интеллекта в правоотношениях – лишь вопрос времени.

О наделении в перспективе роботов особым правовым статусом говорится как в публицистике, так и в правовых актах. Например, в Резолюции Европарламента от 16 февраля 2017 г. № 2015/2103 «Нормы гражданского права о робототехнике». Этот документы не имеет юридической силы в России, но может быть использован как ориентир для регулирования правового положения носителей искусственного интеллекта. В нем сказано, что «по меньшей мере наиболее сложно организованные автономные роботы могут наделяться статусом электронных лиц и нести ответственность за причиненный ими ущерб в тех случаях, когда они принимают решения автономно или иным образом самостоятельно взаимодействуют с третьими лицами». Понятие «электронное лицо» получило распространение и сейчас широко используется в том числе в отечественной доктрине цифрового права. Выработаны по крайней мере три подхода к определению правосубъектности электронных лиц.

Первый основан на сопоставлении электронного лица с физическим лицом и фактическом придании носителю искусственного интеллекта правового статуса человека. Существует интересный и неоднозначный опыт приема человекообразного робота по имени София в гражданство Саудовской Аравии. Критики этого подхода обращают внимание на то, что в данном случае робот будет обладать правами человека, такими как право на достоинство, право на неприкосновенность, право на получение вознаграждения за труд. Это противоречит Конвенции о защите прав человека и основных свобод, а также другим актам, основанным на идеологии признания человека, его прав и свобод высшей ценности. Реализация этого

подхода требует не только осознания субъектности электронного лица, но и принципиального пересмотра модели правового статуса личности.

Второй подход исходит из принципиальной возможности определения статуса электронных лиц по аналогии с юридическим лицом. В данном случае применяется прием юридический фикции. Он допускает возможность условного наделения электронных лиц статусом субъектов права с обособленным имуществом, которое формируется человеком – пользователем электронного лица. В этом случае электронное лицо выступает, например, как агент, действующий автономно на основе искусственного интеллекта, но в интересах определенного лица. Например, в сфере биржевой торговли такое электронное лицо может быть обучено для совершения сделок по определенному алгоритму со скоростью, недоступной человеку. Закрепление за ним обособленного имущества, по аналогии с имуществом юридического лица, позволяет решить проблему возмещения убытков, возникших в результате деятельности электронного агента. А признание за ним специальной правоспособности исходя из его функционального назначения обеспечит юридическую силу решений, принимаемых им. Критики этого подхода отмечают, что правовой статус робота не может быть выведен из модели юридического лица, поскольку последний подразумевает существование людей, стоящих за юридическим лицом, которые представляют его и руководят его деятельностью. В случае с роботом это не так.

Третий подход основан на аналогии англосаксонского траста. Однако этот режим чрезвычайно сложен, требует очень специализированных навыков и не решит проблему ответственности. Что еще более важно, такой подход все равно будет подразумевать существование человека – доверительного управляющего – ответственного за управление роботом.

Перечисленные подходы вряд ли можно считать готовыми решениями. Перспективы правового статуса цифровых лиц следует оценивать на основе реалистичного представления о возможностях современного искусственного интеллекта. Вера в его подобие человеческому сознанию основана на переоценке реальных возможностей даже самых продвинутых роботов, поверхностном понимании способности к самообучению, а также неверном восприятии роботов, искаженном научной фантастикой.

Ошибки в оценке возможностей искусственного интеллекта также часто происходят и в сторону их недооценки. Например, в среде юристов часто высказывается упрек в адрес искусственно интеллекта по поводу того, что с его помощью нельзя механизировать девиантное поведение, поскольку технология не может воспроизвести иррациональную природу человека. Это не так. Искусственный интеллект не имеет доступа к абсолютной истине, он учится у людей. И если противоправное поведение оказывается для многих людей нормой, то девиантными могут быть и решения, принимаемые искусственным интеллектом, обученным на опыте таких людей.

3.6. Тестовые задания

1. Содержание конституционного права на цифровую информацию определено:

- в ч. 4 ст. 29 Конституции Российской Федерации;
- в Федеральном законе «Об информации, информатизации и защите информации»;
- в четвертой части Гражданского кодекса Российской Федерации;
- в ч.1 ст. 3 Конституции Российской Федерации.

2. Для целей определения субъекта конституционного права на информацию, каждый – это:

- только гражданин Российской Федерации;
- гражданин Российской Федерации, иностранный гражданин и лицо без гражданства;
- только гражданин Российской Федерации и иностранный гражданин;
- только гражданин Российской Федерации и лицо без гражданства.

3. Обладатель информации – это:

- лицо самостоятельно создавшее информацию;
- лицо получившее фактический доступ к информации;
- информационный посредник, осуществляющий передачу информации;
- пользователь информации.

4. Особенности правового статуса обладателя цифровой информации:

- обусловлены нематериальным характером цифровой информации;
- определяются содержанием исключительного права на результат интеллектуальной деятельности;
- определяются содержанием исключительного права на средство индивидуализации;
- определяют содержание прав и обязанностей по аналогии с гражданско-правовой категорией «титульный владелец».

5. Наличие у лица фактического доступа к информации означает что он:

- обладает правовым статусом обладателя информации;
- обладает правовым статусом обладателя информации при условии, если он осуществляет хранение информации;

- обладает правовым статусом владельца информации;
- обладает правовым статусом обладателя информации при условии, если он самостоятельно создал эту информацию.

6. Информационным посредником может быть признан:
- учредитель средства массовой информации;
- регистратор доменных имен;
- владелец сайта;
- оператор поисковой системы.

7. Деятельность информационных посредников:
- является условием реализации информационных прав другими лицами;
- не влияет на реализацию информационных прав другими лицами;
- изменяет содержание передаваемой информации;
- не требует специального правового регулирования ответственности информационных посредников.

8. Сложность определения субъектов цифровых правоотношений обусловлена:
- пространственной удаленностью участников электронного взаимодействия;
- наличием технической инфраструктуры в качестве посредника между участниками цифровой коммуникации;
- их идентификацией на основе метода «разрешено все, что не запрещено»;
- отсутствием правовых институтов, обеспечивающих презумпцию принадлежности цифровых прав и обязанностей определенному лицу.

9. Идентификация лица состоит в:

- установлении сведений о лице и сопоставлении данных сведений с уникальным идентификатором;
- проверке лица на принадлежность ему идентификатора и установление правомерности владения им;
- наделении лица определенными правами и обязанностями в отношении цифровой информации;
- выдаче лицу открытого ключа усиленной электронной подписи.

10. Аутентификация лица – это:

- проверка лица на принадлежность ему идентификатора и установление правомерности владения им;
- установление сведений о лице и сопоставлении данных сведений с уникальным идентификатором;
- наделение лица определенными правами и обязанностями в отношении цифровой информации;
- выдача лицу аутентичного идентификатора подлинности.

11. При аутентификации лица:

- достигается абсолютная точность установления правомерности владения идентификатором;
- достигается относительный уровень достоверности доказательства установления личности;
- происходит проверка принадлежности лицу идентификатора;
- не требуется идентификатор для установления личности.

12. Выберите условные обозначения факторов аутентификации лица:

- «то, что знаю»;
- «то, что имею»;
- «тот, с кем знаком»;
- «то, чего нет».

13. Фактор «то, что знаю» применяется для аутентификации лица при использовании:

- простой электронной подписи;
- усиленной неквалифицированной электронной подписи;
- усиленной квалифицированной электронной подписи;
- упрощенной электронной подписи.

14. Недостаток простой электронной подписи состоит в том, что она:

- не позволяет подтвердить факт формирования электронной подписи определенным лицом;
- не обеспечивает подлинность передаваемых данных;
- не допускает использование паролей длиннее 8 символов;
- не может быть использована по соглашению между участниками электронного взаимодействия.

15. Информация в электронной форме, подписанная простой электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в случаях, установленных:

- Федеральным законом;
- правовым актом Банка России;
- соглашением между участниками электронного взаимодействия;
- Конституцией Российской Федерации;
- международным договором.

3.7. Список литературы

1. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ // СЗ РФ. – 1994. – № 32. – Ст. 3301.

2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. – 2006. – № 31 (ч. I). – Ст. 3448.

3. Федеральный закон от 18.03.2019 № 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации» // СЗ РФ. – 2019. – № 12. – Ст. 1224.

4. Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» // СЗ РФ. – 2017. – № 20. – Ст. 2901.

5. Постановление Правительства РФ от 23.12.2015 № 1414 «О порядке функционирования единой информационной системы в сфере закупок» // СЗ РФ. – 2016. – № 2 (ч. I). – Ст. 324.

6. Постановление Правительства РФ от 28.08.2017 № 1030 «О системе управления реализацией программы «Цифровая экономика Российской Федерации» // СЗ РФ. – 2017. – № 36. – Ст. 5450.

7. Постановление Правительства РФ от 12.04.2018 № 445 «Об утверждении Правил хранения операторами связи текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи» // СЗ РФ. – 2018. – № 17. – Ст. 2489.

8. Постановление Правительства РФ от 02.03.2019 № 234 «О системе управления реализацией национальной программы «Цифровая экономика Российской Федерации» // СЗ РФ. – 2019. – № 11. – Ст. 1119.

9. Распоряжение Правительства РФ от 30.06.2018 № 1322-р (ред. от 20.10.2021) «Об утверждении формы согласия на обработку персональных данных, необходимых для регистрации гражданина Российской Федерации в единой системе идентификации и аутентификации, и биометрических персональных данных гражданина

Российской Федерации в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации». – URL: https://bit.ly/37Nzx5E (дата обращения: 15.05.2022).

10. Постановление Конституционного Суда РФ от 18.07.2012 № 19-П «По делу о проверке конституционности части 1 статьи 1, части 1 статьи 2 и статьи 3 Федерального закона «О порядке рассмотрения обращений граждан Российской Федерации» в связи с запросом Законодательного Собрания Ростовской области» // Собрание законодательства РФ. – 2012. – 30 июля. – № 31. – Ст. 4470.

11. Постановление Конституционного Суда РФ от 26.10.2017 № 25-П «По делу о проверке конституционности пункта 5 статьи 2 Федерального закона «Об информации, информационных технологиях и о защите информации» в связи с жалобой гражданина А.И. Сушкова» // Собрание законодательства РФ. – 2017. – 6 ноября. – № 45. – Ст. 6735.

12. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения». Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27.12.2006 № 373-ст. – М.: Стандартинформ, 2008.

13. ГОСТ Р 43.0.5-2009 «Информационное обеспечение техники и операторской деятельности. Процессы информационно-обменные в технической деятельности. Общие положения». Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 15.12.2009. № 959-ст. – М.: Стандартинформ, 2010.

14. ГОСТ Р 60.0.0.2-2016 «Роботы и робототехнические устройства. Классификация». Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 29.11.2016 № 1842-ст. – М.: Стандартинформ, 2016.

15. ГОСТ Р 60.0.2.1-2016 «Роботы и робототехнические устройства. Общие требования по безопасности». Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 29.11.2016 № 1843-ст. – М.: Стандартинформ, 2016.

16. Приказ ФНС РФ от 17.02.2011 № ММВ-7-2/168@ «Об утверждении Порядка направления требования о представлении документов (информации) и порядка представления документов (информации) по требованию налогового органа в электронном виде по телекоммуникационным каналам связи» (зарегистрировано в Минюсте РФ 28.03.2011 № 20303). – URL: http://www.nalog.ru/prav_act/3796679 (дата обращения: 01.02.2022).

17. Указание Банка России от 14.11.2016 № 4190-У (ред. от 15.07.2021) «О требованиях к использованию электронных документов и порядке обмена информацией в электронной форме при осуществлении обязательного страхования гражданской ответственности владельцев транспортных средств». – URL: https://bit.ly/3yzQyLM (дата обращения: 01.02.2022).

18. Резолюция Европарламента от 16.02.2017 2015/2013 (INL). – URL: http://robo-pravo.ru/riezoliutsiia_ies (дата обращения: 01.02.2022).

19. Архипов В.В., Наумов В.Б. О некоторых вопросах теоретических оснований развития законодательства о робототехнике: аспекты воли и правосубъектности // Закон. – 2017. – № 5. – С. 157-170.

20. Банк России – Основные направления развития финансовых технологий на период 2018-2020 годов. – URL:

www.cbr.ru/statichtml/file/36231/on_fintex_2017.pdf (дата обращения: 01.02.2022).

21. Гаджиев Г.А. Является ли робот-агент лицом? (Поиск правовых форм для регулирования цифровой экономики // Журнал российского права. – 2018. – № 1. – С. 15-30.

22. Гаджиев Г.А., Войниканис Е.А. Может ли робот быть субъектом права (поиск правовых норм для регулирования цифровой экономики)? // Право. Журнал Высшей школы экономики. - 2018. – № 4. – С. 37.

23. Гурко А. Искусственный интеллект и авторское право: взгляд в будущее // Интеллектуальная собственность. Авторское право и смежные права. – 2017. – № 12. – С. 7-18.

24. Еманова Н.С. Порядок заключения электронного розничного договора купли-продажи // Юрист. – 2015. – № 3. – С. 16-20.

25. Залоило М.В. Искусственный интеллект в праве: научно-практическое пособие / Под ред. д-ра юрид. наук, проф. Д.А. Пашенцева. – М.: Инфотропик Медиа, 2021.

26. Лебединец О.Н. Гражданская правосубъектность: (сущность, значение, содержание и элементы) // Юрист. – 2003. – № 9. – С. 3.

27. Огородов Д.В. Проблемы этической и правовой регламентации систем искусственного интеллекта (робототехники): обзор круглого стола IP Форума. – URL: http://ipcmagazine.ru/reviews/4374-probl-mes-de-r-gulation-thique-et-juridique-des-syst-mes-d-intelligence-artifi cielle-ro-botique (дата обращения: 01.02.2022).

28. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. – Питер, 2019. – С. 786.

29. Понкин И.В., Редькина А.И. Искусственный интеллект и право интеллектуальной собственности // Интеллектуальная собственность. Авторское право и смежные права. – 2018. – № 2. – С. 35-44.

30. Понкин И.В., Редькина А.И. Искусственный интеллект с точки зрения права // Вестник Российского университета дружбы народов. Серия «Юридические наук»». – 2018. – Т. 22. – № 1. – С. 91-109.

31. Примак Т.К., Орлова К.А. Терминологические трудности определения категории «правовой статус» // Вестник Балтийского федерального университета им. И. Канта. Серия: Экономические и юридические науки. – 2012. – № 9. – С. 19-27.

32. Ужов Ф.В. Искусственный интеллект как субъект права // Пробелы в российском законодательстве. – 2017. – № 3. – С. 359.

33. Хабриева Т.Я., Черногор Н.Н. Право в условиях цифровой реальности // Журнал российского права. – 2018. – № 1. – С. 94-98.

34. Ястребов О.А. Дискуссия о предпосылках для присвоения роботам правового статуса «электронных лиц» // Вопросы правоведения. – 2017. – № 1. – С. 189-203.

35. Ястребов О.А. Правосубъектность электронного лица: теоретико-методологические подходы // Труды Института государства и права РАН / Proceedings of the Institute of State and Law of the RAS. – 2018. – Т. 13. – № 2. – С. 36-55.

36. Kosinski M. Facial recognition technology can expose political orientation from naturalistic facial image / M. Kosinski / Nature.com: [сайт]. – 2021. – URL: https://www.nature.com/articles/s41598-020-79310-1.pdf (дата обращения: 15.05.2022).

37. Krausova м A. Intersections between Law and Artificial Intelligence // International Journal of Computer. – 2017. – Vol. 27. – № 1. – P. 59.

38. Kristie Macrakis: Die Stasi-Geheimnisse: Methoden und Technik der DDR-Spionage. Herbig 2009.

39. Schrijver S. de. The Future Is Now: Legal Consequences of Electronic Personality for Autonomous Robots // Who's Who Legal. 2018. – URL: http://whoswholegal.com/news/features/article/34313/ future-now-legal-con-sequenceselectronic-personality-autonomous-robots (дата обращения: 01.02.2022).

40. Solaiman S.M. Legal personality of robots, corporations, idols and chimpanzees: a quest for legitimacy // Artificial Intelligence and Law. – 2017. – Vol. 25. – № 2. – P. 176.

41. Wörterbuch der Staatssicherheit. GVS JHS 001-400/81, herausgegeben vom BStU 1993.

ГЛАВА 4. СУБЪЕКТИВНОЕ ПРАВО НА ЦИФРОВУЮ ИНФОРМАЦИЮ

4.1. Право на поиск и получение цифровой информации

Определив участников цифровых правоотношений перейдем к характеристике их прав и обязанностей.

Снова обратимся к содержанию части 4 статьи 29 Конституции – «каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом». Она указывает на содержание информационных возможностей, охраняемых конституцией – права на поиск, получение, передачу, производство и распространение информации в том числе в цифровой форме. Важное значение имеет и указание на любой, но непременно законный (а значит на самом деле не совсем любой) способ осуществления перечисленных прав. Этот аспект реализации конституционного права на цифровую информацию опять приводит нас к специальному правовому акту – Закону об информации.

Для конкретизации конституционного права на поиск и получение информации в законе сформулировано понятие доступа к ней. Доступ определен как возможность получения информации и ее использования. Для правильного понимания этого правового режима важно, что для признания информации доступной не требуется ее фактическое получение или ознакомление с ее содержанием. Достаточно лишь самой по себе такой возможности.

Например, доступ к цифровой информации будет считаться состоявшимся даже при осуществлении атаки на сайт типа «отказ в обслуживании» (DDoS-атаке). Она заключается в одномоментном обращении множества компьютеров, входящих в бот-сеть, с запросом на доступ к атакуемому сайту. В результате такого неправомер-

ного доступа работа информационной системы блокируется и фактически информацию не получает никто. Но при рассмотрении дел, связанных с DDoS-атаками, суды исходят из того, что атакующая сторона использовала саму возможность доступа, хоть и не завершившуюся получением информации. Поэтому ссылки на то, что злоумышленник фактически не узнал содержание атакуемой компьютерной информации признаются судами несостоятельными.

Потенциальная доступность информации является также основанием для определения пользователя информацией. Оно дано в Федеральном законе «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления». Пользователь – это субъект, осуществляющий поиск информации о деятельности государственных органов и органов местного самоуправления. Следовательно, факт обращения за информацией уже является основанием для признания лица пользователем.

Право на доступ к информации определено в законодательстве России на первый взгляд очень широко. Согласно Закону об информации граждане и организации вправе осуществлять поиск и получение любой информации в любых формах и из любых источников. Однако эта норма дополняется оговоркой, аналогичной конституционной – право на доступ к информации возможен лишь при условии соблюдения требований, установленных федеральными законами.

При этом явно Закон об информации предусматривает лишь те формы реализации права на получение информации, которые связаны с деятельностью органов власти. Это не значит, что право на доступ к информации исчерпывается только этим. Другие случаи реализации права на доступ могут быть предусмотрены иными правовыми актами. В частности, Закон о персональных данных предусматривает право человека на получение информации, касающейся обработки его персональных данных.

Но вернемся к Закону об информации. Он прямо предусматривает следующие формы реализации права на поиск и получение информации:

Во-первых, гражданин (физическое лицо) имеет право на получение от органов публичной власти информации, непосредственно затрагивающей его права и свободы. Организация имеет право на доступ к информации, непосредственно касающейся ее прав и обязанностей.

Во-вторых, государственные органы и органы местного самоуправления обязаны обеспечивать доступ к информации о своей деятельности. Эта обязанность осуществляется в порядке, предусмотренном тремя федеральными законами: «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»; «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» и «О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации».

Законным способом обеспечения доступа к цифровой информации о деятельности государственного или муниципального органа является ее размещение в сети Интернет. Как правило для этого используются официальные сайты соответствующего органа. Нередко возникает вопрос, могут ли быть признаны официальными источниками информации о деятельности органов власти их страницы в соцсетях и аккаунты в мессенджерах? Можно ли принудить представителя российской власти к общению через них? Известность приобрел случай, когда администратор аккаунта Президента Татарстана в «ВКонтакте» заблокировал другого пользователя социальной сети – жителя республики. Тот обжаловал блокировку в судебном порядке на основании того, что на официальном сайте президента в разделе «Контакты» есть ссылка его страницу в соци-

альной сети ВКонтакте. По мнению истца это означало верификацию аккаунта Президента в соцсети и распространение на него требований Федерального закона «Об обеспечении доступа информации о деятельности государственных органов...». Однако принудить Президента общаться с истцом в соцсети в судебном порядке не удалось.

В зарубежной практике встречаются обратные решения – в 2018 году Федеральный апелляционный суд Манхэттена постановил, что президент Д. Трамп не должен блокировать подписчиков своего аккаунта Twitter за критические высказывания. Суд счел, что блокировка пользователей нарушает свободу слова, поскольку президент использует свой аккаунт для официальной деятельности и взаимодействия с общественностью. Предотвращая доступ критиков к информации, президент запрещает им участвовать в обсуждении в пространстве, которое аналогично по своим характеристикам общественному месту. 9 июля 2019 года Апелляционный суд второго округа США подтвердил, что президент США Дональд Трамп не может блокировать аккаунты своих подписчиков в Twitter. Полагаем, что такие решения могут стать ориентиром и для российских законодателей.

Перечень информации, которая должна быть размещена органами публичной власти в сети, определен Федеральным законом «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» от 9 февраля 2009 № 8-ФЗ. Указанная информация предоставляется бесплатно. За предоставление информации по запросу (например по электронной почте) может взиматься плата если объем запрашиваемой и полученной информации превышает 1 мегабайт. По желанию пользователя запрашиваемая информация может быть передана ему непосредственно в государственном органе или органе

местного самоуправления на носителе (на жестком диске, USB-накопителе, дисковом массиве и т.д.).

Общей особенностью доступа к информации о деятельности органов власти является то, что лицо, желающее получить доступ к ней, не обязано обосновывать необходимость ее получения. Она может потребоваться ему для защиты его прав и законных интересов, для использования в научной, публицистической деятельности, в том числе, для критики деятельности самих органов власти. В запросе информации нет необходимости указывать, каким именно образом запрашиваемая информация затрагивает права и свободы, а также обязанности заявителя.

В то же время обязанность органов власти по обеспечению доступа к информации не распространяется на сведения о правовой оценке актов, принятых самим органом, о проведении анализа деятельности органа или проведении иной аналитической работы, непосредственно не связанной с защитой прав пользователя (пп. 6 п.1 ст. 20 Федерального закона от 9 февраля 2009 № 8-ФЗ). То есть доступ гарантируется к информации, которая уже существует и находится в сфере компетенции данного органа.

Критерий доступности цифровой информации используется для ее правовой классификации. Во-первых, определяется информация, доступ к которой не может быть ограничен. К этой категории относятся, в частности нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия органов публичной власти. Так реализуется норма части 3 статьи 15 Конституции РФ – «любые нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, не могут применяться, если они не опубликованы официально для всеобщего сведения». В России в качестве источника официального опубликования правовых актов действует Официальный интернет-

портал правовой информации pravo.gov.ru. С 1 июля 2022 года ему придан статус единого государственного информационно-правового ресурса в Российской Федерации. Тексты правовых актов, с внесенными в них изменениями, размещаемые на pravo.gov.ru, начиная с 1 июля 2022 года являются официальными[39].

Во-вторых, это общедоступная информация. Она состоит из общеизвестных сведений и иной информации, доступ к которой не ограничен. К этой категории относится любая иная информация которая была обнародована ее обладателем. Также общедоступной считается информация для которой установить принадлежность конкретному обладателю не представляется возможным. Любой субъект цифровых отношений может использовать такую информацию по своему усмотрению. При этом следует учитывать, что использование общедоступной информации может быть осуществлено путем ее распространения. А противоправное распространение информации может повлечь юридическую ответственность. Некоторые технологические решения, например, сети на основе протокола Bittorrent при получении информации одновременно приводят к ее распространению. При скачивании файла по умолчанию начинается его раздача. Неосмотрительное использование таких технологий может привести к административной или уголовной ответственности за распространение противоправного контента – экстремистских материалов, порнографии и пр.

В контексте цифровизации важно, что статус общедоступной информации имеют открытые данные. Так называется информация, размещаемая в формате, допускающем автоматизированную обра-

[39] Указ Президента Российской Федерации от 03.03.2022 № 90 «О некоторых вопросах размещения текстов правовых актов на «Официальном интернет-портале правовой информации» (www.pravo.gov.ru)». – URL: https://bit.ly/3uxALdI (дата обращения: 08.07.2022).

ботку без предварительных изменений человеком в целях повторного ее использования. Открытые данные открыты в юридическом, но не в общечеловеческом смысле. Они представляются в специальном формате, предназначенном для машинной обработки – JSON, XML, RDF, Microdata и других. К примеру, не признается информацией в формате открытых данных изображение, полученное в результате обычного сканирования бумажного документа без распознавания изложенного в нем текста. Открытыми данными такой документ станет при условии распознавания текста, перевода его в форму цифрового документа, разметки для автоматизированной обработки и размещения в сети. Поэтому открытые данные на первый взгляд практически бесполезны для человека, но их машинная обработка может привести к получению результатов, обладающих большой экономической и научной ценностью. Юридические вопросы обработки открытых данных мы рассмотрим в специальной части курса, посвященной регулированию больших данных.

Третья категория цифровых данных по критерию их доступности – информация ограниченного доступа, к которой относится государственная тайна, а также иная конфиденциальная информация.

4.2. Право на предоставление и распространение цифровой информации

Понятия «представление» и «распространение» применительно к информации разграничены в зависимости от круга лиц, получающих доступ к ней. Информация предоставляется определенному лицу, а распространение происходит в отношении неограниченного круга лиц. Например, отправка электронного сообщения пользователю мессенджера или определенному пользователю сервиса электронной почты является предоставлением цифровой информации. В то же время информация, размещенная на сайте может находиться как в режиме распространения, так и предоставления.

Если для доступа к ней требуется регистрация в качестве лица, обладающего определенным статусом, то это следует считать предоставлением. Если она доступна без регистрации происходит распространение. Предоставление информации по общему правилу осуществляется в порядке, который устанавливается соглашением лиц, участвующих в обмене информацией.

Распространение информации для всеобщего сведения может оказать влияние на более широкий круг лиц, чем предоставление, поэтому требует более детального регулирования. К распространению данных в цифровой форме применяются общие требования, установленные законодательством для оборота информации. В частности, запрещается распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

В то же время, цифровая информация отличается высокой потенцией к распространению и другими качествами, делающими ее чувствительной для личности, общества и государства. Поэтому к ней предъявляются специальные требования. В частности, требуется идентификация обладателя информации. Владелец любого сайта в сети Интернет обязан разместить на принадлежащем ему сайте информацию о своих наименовании, месте нахождения и адресе, адресе электронной почты для направления заявления о нарушении авторских и (или) смежных прав, а также вправе предусмотреть возможность направления этого заявления посредством заполнения электронной формы на сайте. Однако в настоящее время конкретные меры ответственности за неразмещение на сайте информации о владельце для физических лиц и организаций пока не установлены.

Более серьезные правовые меры предпринимаются для обеспечения достоверности цифровой информации. Во-первых, частью 1

ст. 15.3 Закона об информации предусмотрено ограничение доступа к недостоверной общественно значимой информации, распространяемой в сети под видом достоверных сообщений. Это происходит если распространение такой информация создает:

- угрозу причинения вреда жизни, здоровью граждан их имуществу;
- угрозу массового нарушения общественного порядка и общественной безопасности;
- угрозу создания помех функционированию или прекращения функционирования объектов жизнеобеспечения, транспортной или социальной инфраструктуры, кредитных организаций, объектов энергетики, промышленности или связи.

Во-вторых, Уголовный кодекс и законодательство об административных правонарушениях также запрещают распространение заведомо ложной цифровой информации, если ей придан вид достоверных сообщений. Уголовное наказание предусмотрено за публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан, о мерах по обеспечению безопасности населения и территорий. Также уголовное наказание предусмотрено за публичное распространение любой заведомо ложной общественно значимой информации, повлекшее тяжкие последствия (ст. 207.1 и 207.2 УК). Эти нормы были введены Федеральным законом от 01.04.2020 г., что позволяет связать их появление с противодействием информационным последствиям пандемии коронавирусной инфекции.

В 2022 году в связи с необходимостью противодействия распространению недостоверной информации о специальной военной операции на территории Украины уголовный закон был дополнен статьей 207.3. «Публичное распространение заведомо ложной информации об использовании Вооруженных Сил Российской Феде-

рации, исполнении государственными органами Российской Федерации своих полномочий». Запрещено публичное распространение под видом достоверных сообщений заведомо ложной информации, содержащей данные об использовании Вооруженных Сил Российской Федерации в целях защиты интересов Российской Федерации и ее граждан, поддержания международного мира и безопасности, а равно содержащей данные об исполнении государственными органами Российской Федерации своих полномочий за пределами территории Российской Федерации в указанных целях.

Первым по статье о дискредитации российской армии стал приговор депутату муниципального округа Красносельский города Москва Алексею Горинову. В июле 2022 года он был приговорен к семи годам лишения свободы. Согласно материалам дела, на заседании представительного органа местного самоуправления 15 марта 2022 г. А. Горинов заявил, что развлекательный досуг для москвичей недопустим, так как «на территории соседнего суверенного государства ведутся боевые действия»[40].

Публичный характер распространения заведомо ложной информации может проявляться в использовании для этого информационно-телекоммуникационных сетей, в том числе мессенджеров (WhatsApp, Viber и других), в массовой рассылке электронных сообщений абонентам мобильной связи. Наказание может быть назначено как автору такой информации, так и лицу, повторяющему поступившие ему сведения (например, сделавшему репост). Однако в последнем случае необходимо установить, что лицо, сделавшее репост, сознавало, что размещенная им информация является ложной, и имело цель довести эту информацию до сведения других лиц. О придании ложной информации вида достоверной могут свидетель-

[40] В России вынесли первый приговор по статье о дискредитации ВС РФ. – URL: https://bit.ly/3yO5hRE (дата обращения: 16.07.2022).

ствовать, например, формы, способы ее изложения – ссылки на компетентные источники, высказывания публичных лиц, использование поддельных документов, видео- и аудиозаписей либо документов и записей, имеющих отношение к другим событиям.

Аналогичные составы административных правонарушений предусмотрены пп. 9-11 статьи 13.15 Кодекса об административных правонарушениях.

Следует учесть, что перечисленные нормы допускают широкое усмотрение правоохранительных органов. Теоретически под определение недостоверной общественно значимой информации может попасть и недостаточно точный прогноз погоды.

Например, для привлечения к административной ответственности главного редактора сайта «ЭХО Москвы» в марте 2020 года оказалось достаточно того, что в опубликованном интервью о COVID-19, содержалась информация существенно противоречащая данным органов публичной власти. В интервью политолог Валерий Соловей заявил, что «в РФ имеется порядка 1,6 тыс. подтвержденных случаев смерти людей от коронавируса с середины января 2020 года, а количество инфицированных оценивается в 130–180 тыс.». В то же время, по данным оперативного штаба по противодействию распространению инфекции, в тот день в России было зафиксировано всего 93 случая заражения и ни одного смертельного случая.

4.3. Ограничение права на распространение цифровой информации

Особого внимания заслуживают правила ограничения доступа к сайтам в сети Интернет. Судебной практикой признано, что лицом, чьи права, свободы и законные интересы затрагиваются в результате блокировки, прежде всего является распространитель информации – администратор доменного имени, а также владелец

сайта. Поэтому мы рассматриваем этот вопрос в контексте реализации права на распространение информации, а не на доступ к ней. При этом следует учитывать, что в результате запретительных мер ограничивается также конституционное право на поиск и получение информации.

В Российской Федерации ведется своего рода государственный «черный список» сайтов, содержащих запрещенную информацию – Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты, содержащие информацию, распространение которой в Российской Федерации запрещено.

Как следует из названия реестра, блокировка сайтов может осуществляться по-разному. Во-первых, по доменному имени или URL страницы. У этого способа есть побочный эффект – при работе сайта по протоколу HTTPS блокировка хотя бы одной его страницы приводит к недоступности сайта в целом. Во-вторых, по сетевому адресу (IP), что потенциально может привести к блокировкам ресурсов добросовестных обладателей информации, находящейся на том же узле (сервере), а также может быть неэффективно в силу простоты смены IP-адреса.

Решение о блокировке информационного ресурса принимается либо в административном порядке уполномоченным органом исполнительной власти или органами Прокуратуры либо судом.

Не требуется судебного решения для ограничения доступа к детской порнографии, информации о наркотических средствах, о способах совершения самоубийства, несовершеннолетнем, пострадавшем в результате противоправных действий, о незаконных азартных играх, продаже алкоголя через Интернет, незаконной торговле лекарствами и др. Также в административном порядке ограничивается информация, направленная на вовлечение несовершен-

нолетних в совершение противоправных действий, представляющих угрозу для их жизни и здоровья либо для жизни и здоровья иных лиц. Перечень запрещенной для распространения через Интернет информации постоянно расширяется.

Вопреки бытующему мнению, блокировка перечисленной информации происходит не только по решению Роскомнадзора. Этот вопрос находится в компетенции и других органов власти – МВД борется с порнографией и оборотом наркотиков, Роспотребнадзор – с пропагандой суицида, Росалкогольрегулирование – с незаконной продажей алкоголя, Федеральная налоговая служба – с нелегальными онлайн-казино. Противодействие информации, опасной для детей, осуществляет Росмолодежь. Если решение принимается перечисленными органами, Роскомнадзор лишь обеспечивает их организационно-техническое исполнение. Поводом для оценки информации на ее соответствие закону является обращение, которое любой гражданин или организация могут направить через форму на сайте Роскомнадзора.

Также Закон об информации специально предусматривает особый порядок ограничения наиболее опасной для государства информации – призывов к массовым беспорядкам, экстремистской деятельности, участию в незаконных публичных мероприятиях, а также недостоверной общественно значимой информации и материалов организаций, признанных нежелательными. Она блокируется Роскомнадзором по обращению Генерального прокурора или его заместителей.

В судебном порядке может быть запрещена к распространению любая другая информация, помимо перечисленной выше. Теоретически запрещена может быть любая информация, если ее распространение будет признано судом противоправным. Судебный порядок в теории должен предоставлять большие гарантии обладателю информации. Но в действительности он мало чем отличается от

принятия аналогичного решения в административном порядке. По данным Судебного департамента при Верховном Суде Российской Федерации за 2019 год, судами было рассмотрено примерно 60 тысяч дел данной категории, решение о признании информации запрещенной вынесено в 99% случаях.

Суды признают запрещенной информацию самого разного рода, например, о продаже дипломов об окончании высших учебных учреждений, медицинских справок различных видов, фальшивых денег. В последнее время большие усилия судебных органов направлены на ограничение информации об аниме. За 2021 год Роскомнадзор добился удаления около двух тысяч ссылок на сайты с аниме-сериалами или мультипликационными произведениями. В 2020 году таких блокировок не было.

Интересно, что в связи с отсутствием единообразия судебной практики распространение сходной информации может быть как законным, так и противоправным. Непростая судьба у многих сайтов с информацией о криптовалютах. Суды часто удовлетворяют требования прокуроров о запрете информации о возможности использования в качестве средства платежа «электронной валюты Bitcoin (биткоин)». В обоснование требований обычно указывается, что криптовалюта не обеспечена реальной стоимостью и не содержит информации о ее держателях. Процесс выпуска и обращения криптовалюты полностью децентрализован и отсутствует возможность его регулирования, в том числе со стороны государства. По мнению органов прокуратуры, это противоречит Законам о Центральном банке Российской Федерации и об информации. Суды исходят из того, что распространение такой информации противоречит запрету на введение на территории РФ других денежных единиц, помимо российского рубля, и выпуск денежных суррогатов. В других судебных решениях такая позиция опровергается. Суды отмечают, что доводы об отнесении криптовалюты к денежным суррогатам могут

быть признаны имеющими лишь предположительный характер, а распространение информации о цифровых финансовых активах или общей информации о криптовалюте законодательством РФ не запрещено.

4.4. Право на забвение

Обзор права на цифровую информацию был бы неполным без изучения новых правовых возможностей, неизвестных ранее. Их осознание связано с особенностями оборота цифровой информации.

Поисковые системы играют определяющую роль в формировании повседневной информационной повестки как для каждого отдельного человека, так и для всего общества. Информация, отсутствующая в результатах поиска Google или Yandex с очень высокой вероятностью останется неизвестной. На понимании этой закономерности основано так называемое права на забвение. Само по себе оно не является конституционным, авторы Конституции в 1993 году не могли осознать важную роль поисковых систем, поскольку тогда их просто не существовало. Оно основано на сочетании других конституционных ценностей – права на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени (ч. 1 ст. 23 Конституции), а также на недопустимости сбора, хранения, использования и распространения информации о частной жизни лица без его согласия (ч.1 ст. 24).

Право на забвение определено законом об информации как обязанность оператора поисковой системы по требованию гражданина (физического лица) прекратить выдачу ссылок, ведущих к информации о нем. Это требование должно быть исполнено не только, если информация распространяется с нарушением законодательства Российской Федерации или является недостоверной. Удалению также подлежат ссылки на неактуальную информацию, утратившую значение для заявителя в силу последующих событий или

действий заявителя. При этом право на забвение не касается информации о событиях, содержащих признаки уголовно наказуемых деяний, сроки привлечения к уголовной ответственности по которым не истекли, и информации о совершении гражданином преступления, по которому не снята или не погашена судимость.

Требование заявителя должно содержать:

1) фамилию, имя, отчество, паспортные данные, контактную информацию (номера телефона и (или) факса, адрес электронной почты, почтовый адрес);

2) информацию о заявителе, выдача ссылок на которую подлежит прекращению;

3) указатель страницы сайта в сети Интернет, на которой размещена информация;

4) основание для прекращения выдачи ссылок поисковой системой;

5) согласие заявителя на обработку его персональных данных.

В течение десяти рабочих дней с момента получения требования заявителя оператор поисковой системы обязан прекратить выдачу ссылок на информацию или направить заявителю письменный отказ. Заявитель, считающий отказ оператора поисковой системы необоснованным, вправе обратиться в суд.

Для ослабления эффекта Стрейзанд законом предусмотрена обязанность оператора поисковой системы не раскрывать информацию о факте обращения к нему заявителя. Однако информация о реализации права на забвение может стать публичной в случае, если дело дойдет до суда. В таком случае информация, доступ к которой пытается ограничить гражданин, с высокой вероятностью станет общеизвестной.

Удовлетворение требования гражданина не означает удаления спорной информации: доступ к ней возможен при обращении непосредственно к конкретному сайту, где эта информация размещена.

Право на забвение позволяет соблюсти разумный баланс между правом на уважение частной жизни такого лица и правом на доступ к информации о нем неопределенного круга лиц, которое также имеет конституционную природу.

4.5. Право на анонимность

Цифровая коммуникация обеспечивает возможность общения людей, находящихся далеко друг от друга. С одной стороны, удаленность пользователей в пространстве и общение через техническую инфраструктуру создает ощущение анонимности сетевого общения. С другой, проникновение сетевых технологий практически во все сферы общественной и личной жизни означает объективную необходимость обеспечения конфиденциальности чувствительных для личности цифровых данных. Уровень конфиденциальности должен быть по крайней мере не ниже конституционных стандартов, определенных еще для «аналоговой» информации. Необходимость приспособления классических правовых конструкций к цифровой реальности способствовала широкому распространению движения за право на анонимность общения в сети.

При этом необходимо учесть то, что в действительности право на анонимность в Интернете пока в правовых актах не определено. Аргументы в пользу его закрепления в какой-то степени могут быть выведены из положения Конституции о том, что «каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения». Согласно сложившейся практике под иными сообщениями понимаются в том числе электронные – например СМС- и ММС-сообщения, факсимильные сообщения, передаваемые посредством сети «Интернет» мгновен-

ные сообщения, электронные письма, видеозвонки, а также сообщения, пересылаемые иным способом. То есть тайна связи распространяется и на цифровые данные.

Закон о персональных данных также запрещает раскрывать персональные данные третьим лицам и распространять их без согласия субъекта этих данных. Аналогичные положения содержатся в Законе о связи. Уголовным кодексом предусмотрена ответственность за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан. Проведение оперативно-розыскных мероприятий, включая получение компьютерной информации, которые ограничивают конституционные права человека и гражданина на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, а также право на неприкосновенность жилища, допускается на основании судебного решения.

В то же время Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы, утвержденная Указом Президента Российской Федерации от 09.05.2017 № 203 оценивает анонимность критически. Она предусматривает выработку системы доверия в сети, «исключающую анонимность, безответственность пользователей и безнаказанность правонарушителей в сети Интернет». В настоящее время в России доминирует движение в направлении ограничения анонимного общения.

Для формирования правовой основы ограничительных мер в 2014 году было введено понятие организатора распространения информации. Под его определение может подпасть практически любое лицо, осуществляющее деятельность в интернете – мессенджеры, социальные сети, почтовые сервисы и любые другие сайты, позволяющие пользователям обмениваться сообщениями. Роскомнадзор ведет реестр организаторов распространения информации, в

который внесены практически все крупнейшие российские интернет-ресурсы и сервисы (Яндекс, ВКонтакте, Mail.Ru, Одноклассники, службы знакомств и другие сайты). С 1 июля 2018 года организаторы распространения информации по так называемому Закону Яровой обязаны хранить на территории России метаданные сообщений и сами электронные сообщения.

Метаданные – это информация о фактах приема, передачи, доставки и обработки электронных сообщений пользователей и информацию об этих пользователях. Проводя аналогию с обычной перепиской можно сказать, что метаданные – это электронный аналог того, что написано на конверте – адреса, информация об отправителе и получателе, почтовые отметки.

Также сохраняется содержание переписки пользователей – текстовые сообщения, голосовая информация, изображения, звуки-, видео-, иные электронные сообщения. Они должны храниться до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки. То есть продолжая аналогию с бумажной перепиской, храниться должен и конверт с отметками, и письмо из этого конверта.

Организатор распространения информации обязан не просто хранить перечисленную информацию, но и предоставлять ее органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации. Если для обеспечения тайны электронной коммуникации используется шифрование, также предоставляется информация, необходимая для декодирования сообщений. Несоблюдение этой обязанности является административным правонарушением и основанием для блокировки информационного ресурса организатора распространения информации в сети Интернет. Отказ от предоставления ключей шифрования был основанием для ограничения доступа к Telegram в 2018 году.

С марта 2022 года также вводятся специальные требования об идентификации пользователей мессенджеров. Обязанность организатора сервиса обмена мгновенными сообщениями осуществлять идентификацию пользователей установлена статьей 10.1 Закона об информации. Правила идентификации утверждены Постановлением Правительства Российской Федерации от 20.10.2021 № 1801, они вступают в силу с 1 марта 2022 года. Идентификация пользователей мессенджеров будет осуществляться с помощью номера мобильного телефона пользователя. Проверка принадлежности номера конкретному лицу проходит по двум каналам. Во-первых, для подтверждения номера администратор мессенджера предлагает пользователю совершить действия с использованием этого номера (например, ввести пин-код, отправленный через смс). Во-вторых, сведения о принадлежности номера определенному лицу обязан подтвердить оператор мобильной связи. Если проверка не пройдена, администратор мессенджера обязан не допускать передачу электронных сообщений пользователем.

Предложенный порядок не свободен от недостатков. Помимо очевидного наступления на интересы сторонников анонимного общения в сети, порядок не отвечает на два принципиальных вопроса – как будет осуществляться идентификация пользователей, не имеющих номеров мобильной связи и как обеспечить исполнение порядка зарубежными администраторами мессенджеров, находящимися вне действия российского права. На первый вопрос ответа пока нет, на второй возможно ответит практика применения Федерального закона «О деятельности иностранных лиц в информационно-телекоммуникационной сети Интернет на территории Российской Федерации» от 1 июля 2021 г. № 236-ФЗ. Мы уже подробно разбирали его нормы при изучении вопроса о действии цифрового права в пространстве.

4.6. Тестовые задания

1. Информация находится в правовом режиме доступа в случае:
- её фактического получения;
- ознакомления с ее содержанием;
- наличия возможности ее получения и использования;
- ее фактического использования.

2. Правовой статус пользователя информации имеет:
- гражданин, осуществляющий поиск информации;
- лицо, распространяющее информацию;
- гражданин, получивший фактический доступ к информации;
- субъект Российской Федерации.

3. Федеральный закон «Об информации, информационных технологиях и защите информации» предусматривает право гражданина на получение:
- информации о деятельности органов государственной власти через официальные аккаунты должностных лиц в сервисах обмена мгновенными сообщениями (мессенджерах);
- информации, непосредственно затрагивающей права и свободы гражданина;
- информации о деятельности органов местного самоуправления при условии обоснования гражданином необходимости ее получения;
- информации от органа государственной власти о правовой оценке актов, принятых им.

4. Информация на странице сайта, доступной для неопределенного круга лиц, находится в правовом режиме:
- распространения;
- предоставления;

- владения;
- собственности.

5. Ч. 1 ст. 15.3 Федерального закона «Об информации...» предусмотрено ограничение доступа к:

- любой недостоверной общественно значимой информации;
- любой недостоверной общественно значимой информации, распространяемой в сети под видом достоверных сообщений;
- недостоверной общественно значимой информации распространяемой в сети под видом достоверных сообщений, если распространение такой информация создает угрозу причинения вреда жизни, здоровью граждан их имуществу;
- недостоверной общественно значимой информации распространяемой в сети под видом достоверных сообщений, если распространение такой информация создает угрозу нарушения конфиденциальности персональных данных граждан Российской Федерации.

6. Не требуется решение суда для ограничения доступа к страницам сайтов в сети «Интернет», содержащим информацию:

- о способах совершения самоубийства;
- о криптовалютах;
- утратившую значение для гражданина в силу последующих событий;
- не соответствующую действительности.

7. Право на забвение заключается в:

- обязанности оператора поисковой системы по требованию физического лица прекратить выдачу ссылок, ведущих к информации о нем;
- обязанности оператора поисковой системы по требованию физического или юридического лица прекратить выдачу ссылок, ведущих к информации о нем;

- праве физического лица требовать удаления из сети Интернет информации о событиях, содержащих признаки уголовно наказуемых деяний;
- праве юридического лица требовать удаления из сети Интернет информации, порочащей его деловую репутацию.

8. Право на анонимность:
- пока не имеет законодательного закрепления;
- закреплено в Федеральном законе «Об информации, информационных технологиях и защите информации»;
- закреплено в Федеральном законе «Об информации, информатизации и защите информации»;
- определено в четвертой части Гражданского кодекса Российской Федерации.

9. Конституционное право на тайну связи:
- распространяется только на телефонные переговоры, почтовые отправления и телеграфные сообщения;
- распространяется только на переписку, телефонные переговоры, почтовые отправления и телеграфные сообщения;
- распространяется только на переписку, телефонные переговоры, почтовые отправления и телеграфные сообщения;
- распространяется на переписку, телефонные переговоры, почтовые отправления, телеграфные и иные, в том числе электронные, сообщения.

10. Согласно Постановлению Правительства Российской Федерации от 20.10.2021 № 1801 идентификация пользователей сервиса обмена мгновенными сообщениями осуществляется с помощью:
- номера мобильного телефона;
- паспорта гражданина Российской Федерации;
- СНИЛС;
- ИНН.

4.7. Список литературы

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. – 2006. – № 31 (ч. I). – Ст. 3448.

2. Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» // СЗ РФ. – 2017. – № 20. – Ст. 2901.

3. Постановление Правительства РФ от 23.12.2015 № 1414 «О порядке функционирования единой информационной системы в сфере закупок» // СЗ РФ. – 2016. – № 2 (ч. I). – Ст. 324.

4. Постановление Правительства РФ от 28.08.2017 № 1030 «О системе управления реализацией программы «Цифровая экономика Российской Федерации» // СЗ РФ. – 2017. – № 36. – Ст. 5450.

5. Постановление Правительства РФ от 12.04.2018 № 445 «Об утверждении Правил хранения операторами связи текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи» // СЗ РФ. – 2018. – № 17. – Ст. 2489.

6. Постановление Правительства РФ от 02.03.2019 № 234 «О системе управления реализацией национальной программы «Цифровая экономика Российской Федерации» // СЗ РФ. – 2019. – № 11. – Ст. 1119.

7. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения». Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27.12.2006 № 373-ст. – М.: Стандартинформ, 2008.

8. ГОСТ Р 43.0.5-2009 «Информационное обеспечение техники и операторской деятельности. Процессы информационно-обменные в технической деятельности. Общие положения». Утвер-

жден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 15.12.2009. № 959-ст. – М.: Стандартинформ, 2010.

9. Винья П., Кейси М. Эпоха криптовалют: как биткоин и блокчейн меняют мировой экономический порядок / пер. с англ. Э. Кондуковой; науч. ред. А. Форк. – М.: Манн, Иванов и Фербер, 2017.

10. Генкин А., Михеев А. Блокчейн: как это работает и что ждет нас завтра. – М.: Альпина Паблишер, 2018. – 592 с.

11. Институты и путь к современной экономике. Уроки средневековой торговли / пер. с англ. И. Кушнаревой. – М.: Изд. дом Высшей школы экономики, 2013 (Экономическая теория).

12. Защита данных: научно-практический комментарий к судебной практике / В.В. Лазарев, Х.И. Гаджиев, Э.В. Алимов [и др.]; отв. ред. В.В. Лазарев, Х.И. Гаджиев; Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации. – М.: ООО «ЮРИДИЧЕСКАЯ ФИРМА КОНТРАКТ», 2020. – 176 с.

13. Лапидус Л.В. Цифровая экономика: управление электронным бизнесом и электронной коммерцией: монография. – М.: ИНФРА-М, 2018. – 381 с.

14. Мохат П.М. Искусственный интеллект. Правовой взгляд. – М., 2017.

15. Нагродская В.Б. Новые технологии (блокчейн / искусственный интеллект) на службе права: научно-методическое пособие / под ред. Л.А. Новоселовой. – М.: Проспект, 2019. – 128 с.

16. Новые законы робототехники. Регуляторный ландшафт. Мировой опыт регулирования робототехники и технологий искусственного интеллекта / [В. Бакуменко и др.]; под ред. А.В. Незнамова. – М.: Инфотропик Медиа, 2018.

17. Основы государственной политики в сфере робототехники и технологий искусственного интеллекта / [А. Бутримович и др.]; под ред. А.В. Незнамова. – М.: Инфотропик Медиа, 2019. – 184 с.

18. Правовое регулирование экономических отношений в современных условиях развития цифровой экономики: монография / А.В. Белицкая, В.С. Белых, О.А. Беляева [и др.]; отв. ред. В.А. Вайпан, М.А. Егорова. – М.: Юстицинформ, 2019.

19. Правовое регулирование цифровой экономики в современных условиях развития высокотехнологичного бизнеса в национальном и глобальном контексте: коллективная монография / Под общ. ред. В.Н. Синюкова, М.А. Егоровой. – М.: Проспект, 2019.

20. Регулирование робототехники: введение в «робоправо». Правовые аспекты развития робототехники и технологий искусственного интеллекта / [В.В. Архипов и др.]; под ред. А.В. Незнамова. – М.: Инфотропик Медиа, 2018. – 232 с.

21. Самолысов П.В. Информатизация образования. Избранные научные труды: монография. – М.: АИО, 2011. – 188 с.

22. Сырых В.М. Теория государства и права: учебник. – М.: Юстицинформ, 2012. – 704 с.

23. Халфина Р.О. Общее учение о правоотношении. – М., 1974. – 126 с.

Учебное издание

Волков Владислав Эдуардович

ЦИФРОВОЕ ПРАВО. ОБЩАЯ ЧАСТЬ

Учебное пособие

Редакционно-издательская обработка А.В. Ярославцевой
Компьютерная вёрстка А.В. Ярославцевой

Подписано в печать 17.08.2022. Формат 60×84 1/16.
Бумага офсетная. Печ. л. 7,0.
Тираж 25 экз. Заказ № . Арт. – 2(Р2У)/2022.

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САМАРСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА С. П. КОРОЛЕВА»
(САМАРСКИЙ УНИВЕРСИТЕТ)
443086, САМАРА, МОСКОВСКОЕ ШОССЕ, 34.

Издательство Самарского университета.
443086, Самара, Московское шоссе, 34.