
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В РОССИИ



**BEITEN
BURKHARDT**

СОДЕРЖАНИЕ

1. Правовое регулирование	4
2. Цифровые права	4
3. Закон об изоляции Рунета	5
4. Заключение договоров через Интернет	5
5. Ограничения в отношении закупок иностранного программного обеспечения	6
6. Ограничение работы анонимайзеров и сервисов VPN	8
7. Организация распространения информации в сети Интернет	8
8. Право на забвение	9
9. Локализация персональных данных	9
10. Иные основания для блокировки сайтов	10
11. Сотрудничество с иностранными партнерами	11
12. Меры государственной поддержки ИТ-индустрии	12

1. Правовое регулирование

Основным документом, регламентирующим использование информационных технологий в России, является Федеральный закон от 27.07.2006 № 149-ФЗ “Об информации, информационных технологиях и о защите информации” (далее – “**Закон об информации**”). Указанный закон, в частности, определяет основной понятийный аппарат в рамках использования сети Интернет, а также устанавливает основные ограничения в отношении пользования Интернетом.

В дополнение к Закону об информации отдельные аспекты деятельности, предполагающей использование информационных технологий, также регулируются профильным законодательством, в частности, Гражданским Кодексом РФ (далее – “**ГК РФ**”), федеральными законами “О рекламе”, “О защите конкуренции”, “О персональных данных”, “О защите прав потребителей”, “О связи”.

Основным государственным органом, осуществляющим контроль и надзор в сфере информационных технологий, является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций – Роскомнадзор. Однако в последнее время все больше полномочий в данной сфере получает и Федеральная служба безопасности (ФСБ).

2. Цифровые права

С 01 октября 2019 года вступит в силу статья 141.1 ГК РФ, которой вводится понятие цифровых прав. Однако, цифровым правам дается лишь самое общее определение, при этом конкретные виды таких прав, их содержание и условия их осуществления ещё должны быть определены законодательством. В этой связи, в частности, ожидается появление более детального регулирования по результатам рассмотрения законопроекта № 419059-7 “О цифровых финансовых активах”.

3. Закон об изоляции Рунета

С 01 ноября 2019 года вступает в силу Федеральный закон от 1 мая 2019 г. № 90-ФЗ, вносящий изменения в Федеральный закон “О связи” и Закон об информации, который устанавливает ряд новых обязанностей для операторов связи и владельцев сетей связи, в частности:

- выполнять требования в части обеспечения устойчивого функционирования средств связи и использования определенных точек обмена трафиком (такие требования должны быть установлены Роскомнадзором);
- обязанность операторов связи установить технические средства противодействия угрозам целостности, устойчивости и безопасности функционирования сети Интернет.

Целью закона заявлено обеспечение возможности автономного функционирования российского сегмента сети Интернет при возникновении внешних угроз. В то же время, у российских пользователей вызывает опасения возможность использования закона в целях ограничения использования информации, размещённой за пределами России. Тем не менее, закон содержит значительное количество отсылочных норм, и его практическое применение будет зависеть от содержания подзаконных актов, которые должны быть приняты в целях его исполнения.

4. Заключение договоров через Интернет

Долгое время заключение договоров через сеть Интернет без использования электронной подписи не имело специального регулирования. Формально это не препятствовало совершению сделок на основании общих положений законодательства о форме сделки, однако могло вызвать сложности с доказыванием содержания совершенной сделки при возникновении споров, поскольку содержание сделки не было закреплено документально.

С учетом стремительно растущего объема таких сделок (особенно в секторе B2C), вопрос о порядке заключения договоров через Интернет был, наконец, законодательно урегулирован – с 01 октября 2019 года вступают в силу изменения в статьи 160 и 434 ГК РФ о письменной форме сделки и форме договора.

Статья 160 ГК РФ дополнена абзацем, согласно которому письменная форма сделки также будет считаться соблюденной в случае совершения лицом сделки с помощью электронных средств в случае, если возможно установить содержание такой сделки на материальном носителе. При этом требование о наличии подписи будет считаться

выполненным, если использован любой способ, позволяющий достоверно определить лицо, выразившее волю (специальный способ может быть предусмотрен законом или соглашением сторон).

Кроме того, статья 434 ГК РФ дополняется положением о возможности заключения договора путем составления одного электронного документа или посредством обмена электронными документами в соответствии с описанными выше новыми положениями статьи 160 ГК РФ.

Необходимо отметить, что в отношении лицензионных договоров с конечными пользователями программ для ЭВМ (так называемых end-user license agreement – EULA) уже несколько лет действует особый порядок их заключения, в соответствии с которым условия такой лицензии могут быть изложены в электронном виде, а начало использования программы пользователем означает согласие на заключение договора (пункт 5 статьи 1286 ГК РФ).

5. Ограничения в отношении закупок иностранного программного обеспечения

В настоящее время в России действует запрет на закупки программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд. Указанный запрет напрямую касается только закупок, осуществляемых государственными и муниципальными субъектами и органами власти. Однако уже сейчас многие компании с государственным участием добровольно применяют указанное ограничение и не исключено, что запрет на закупку иностранного программного обеспечения будет распространен на указанные компании в будущем.

Содержание запретительных мер, изначально введенных Постановлением Правительства РФ от 16.11.2015 № 1236, было изменено с 1 января 2018 года. В частности, теперь они не распространяются на программное обеспечение, происходящее из стран Евразийского экономического союза и включенное в соответствующий реестр. Кроме того, в настоящее время запрет касается не только прямого приобретения программного обеспечения (лицензий на него), но и иных способов предоставления программного обеспечения, включая поставку оборудования, на которую программное обеспечение подлежит установке в результате исполнения контракта.

В отношении применения указанного запрета установлены два исключения, когда иностранное программное обеспечение все-таки может быть приобретено для государственных или муниципальных нужд, а именно: (1) если в реестре российского программного обеспечения (или в реестре евразийского программного обеспечения) отсутствуют сведения о программном обеспечении необходимого класса либо (2) программное обеспечение такого класса имеется в соответствующих реестрах, но по своим функциональным, техническим или эксплуатационным характеристикам не соответствует установленным заказчиком требованиям.

Для включения в реестр российского программного обеспечения исключительное право на соответствующий продукт на территории всего мира должно принадлежать российской организации без преобладающего иностранного участия (меньше 50%). Кроме того, общая сумма выплат за использование объектов интеллектуальной собственности и/или выполнение работ (оказание услуг) по разработке, модификации и адаптации программного обеспечения в адрес иностранных лиц, их представителей и контролируемых ими российских организаций должна составлять менее 30% выручки правообладателя, полученной им за календарный год в качестве вознаграждения за предоставление права использования программы.

Аналогичные требования предъявляются и для включения в реестр евразийского программного обеспечения (с поправкой на принадлежность организаций и/или граждан к государствам-членам Евразийского экономического союза).

В настоящее время в реестре российского программного обеспечения зарегистрировано свыше 5.200 программных продуктов, тогда как реестр евразийского программного обеспечения еще не сформирован.

Ранее в СМИ анонсировалось создание в 2017 году аналогичного реестра российского ИТ-оборудования, однако до настоящего времени эта идея не была реализована.

6. Ограничение работы анонимайзеров и сервисов VPN

01 ноября 2017 года вступили в силу изменения в Закон об информации, обязывающие владельцев анонимайзеров и сервисов VPN обеспечивать соблюдение запретов на доступ к определенным информационным ресурсам.

Роскомнадзор осуществляет поиск владельцев VPN и анонимайзеров и направляет им требования о необходимости подключения к реестру заблокированных ресурсов. При отказе владельца анонимайзера или сервиса VPN от сотрудничества Роскомнадзор, в свою очередь, вправе заблокировать доступ к соответствующим сервисам.

Следует учитывать, что указанные требования относятся к анонимайзерам и сервисам VPN массового использования, в то время как из-под действия закона выведены сервисы, имеющие заранее определенный их владельцами круг пользователей, которые используют их для собственных нужд.

Роскомнадзор начал применять вышеприведенные нормы только в 2019 году, направив требования о подключении к системе заблокированных ресурсов 10 сервисам: NordVPN, Hide My Ass!, Hola VPN, Openvpn, VyprVPN, ExpressVPN, TorGuard, IPVanish, Kaspersky Secure Connection и VPN Unlimited. На текущую дату информация об иностранных сервисах, согласившихся выполнить требования Роскомнадзора, отсутствует, и с высокой степенью вероятности таковых не найдется в дальнейшем.

7. Организация распространения информации в сети Интернет

В соответствии с Законом об информации организаторами распространения информации в сети Интернет являются лица, обеспечивающие функционирование сервисов, предназначенных для приема, передачи, доставки или обработки электронных сообщений пользователей сети Интернет.

Организаторы распространения информации подлежат включению в специальный реестр Роскомнадзора и должны хранить информацию о пользователях, передаваемые ими сообщения и файлы, а также предоставлять указанные данные по запросу компетентных органов, передавать ФСБ ключи для декодирования электронных сообщений и выполнять ряд иных обязанностей. Неисполнение соответствующих обязательств может повлечь за собой блокировку соответствующего информационного ресурса.

Несмотря на первоначальную нацеленность на мессенджеры и социальные сети, фактически под определение “организатор распространения информации” попадают любые сервисы с возможностью обмена сообщениями и иным контентом между пользователями (например, сайт с форумом). Это привело к тому, что в реестре наряду, например, с мессенджерами (WeChat, Threema, Telegram) зарегистрирован сайт психоневрологического интерната.

Из крупных ресурсов ограничению доступа – достаточно безуспешно – в настоящее время подвергается только Telegram, который отказался предоставить ключи ФСБ. При этом множество крупных ресурсов, подпадающих под определение организатора распространения информации (например, WhatsApp, Facebook, сервисы Google), не зарегистрировались в соответствующем реестре и остаются без внимания со стороны Роскомнадзора.

8. Право на забвение

С 01 января 2016 года вступили в силу изменения в Закон об информации, согласно которым любое физическое лицо вправе потребовать от оператора поисковой системы, распространяющего рекламу, направленную на российских потребителей, прекратить выдачу сведений о нем, если такие сведения распространяются с нарушением российского законодательства, являются недостоверными или утратившими актуальность. Исключение составляет информация о преступлениях, в отношении которых не истекли сроки привлечения к ответственности или по которым не снята или не погашена судимость.

9. Локализация персональных данных

С 01 сентября 2015 года в России действует требование по локализации персональных данных, согласно которому лицо, собирающее персональные данные граждан России через сеть Интернет или иным способом, обязано производить все операции с такими данными (в том числе запись, хранение, обновление и извлечение персональных данных) через базы данных, находящиеся на территории Российской Федерации. Введение указанного требования обосновывалось необходимостью защиты персональных данных российских граждан от возможных негативных действий из-за рубежа.

Вместе с тем, продолжают действовать положения законодательства, допускающие трансграничную передачу персональных данных на территории иностранных государств. Согласно разъяснениям, опубликованным на сайте Минкомсвязи РФ, базы данных с персональными данными должны создаваться, обновляться и храниться на территории России, однако в дальнейшем база данных может быть передана за границу. Таким образом, вместо изначально заявленной цели, по сути, требование о локализации баз данных направлено на создание в России соответствующей инфраструктуры для хранения баз данных и обеспечение доступа российских государственных органов к ним.

На текущий момент вследствие несоблюдения требования о локализации персональных данных в России пострадал только один крупный иностранный сервис – Роскомнадзором ограничен доступ к социальной сети LinkedIn. В то же время иные зарубежные сервисы (Facebook, Twitter и т.п.) пока также не выполнили данное требование без каких-либо негативных последствий для себя – в их пользу говорит большая база пользователей в России.

10. Иные основания для блокировки сайтов

Помимо указанных выше случаев ограничения доступа к интернет-сайтам и сервисам при нарушении правил работы анонимайзеров и VPN, нарушении правил работы организаторами распространения информации и операторами персональных данных, российским законодательством предусмотрены и иные основания для блокировки сайтов. Краткая информация о них приведена ниже.

Закон об информации предусматривает ведение единого реестра доменных имен и сетевых адресов сайтов, содержащих запрещенную информацию. Включение сайтов в указанный реестр может осуществляться на основании решения суда, запрещающего распространение соответствующей информации, а также по решению уполномоченного государственного органа в отношении определенных видов информации (например, на основании постановления судебного пристава-исполнителя об ограничении доступа к информации, порочащей честь, достоинство или деловую репутацию гражданина либо деловую репутацию юридического лица).

При включении определенного сайта в реестр провайдер хостинга уведомляет обслуживаемого им владельца данного сайта о необходимости удаления интернет-страницы, содержащей соответствующую информацию, и, если последний не удалил такую страницу, провайдер обязан заблокировать доступ к сайту. Владелец сайта имеет возможность обжаловать решение о включении сайта в указанный реестр в судебном порядке.

С 29 марта 2019 года вступили в силу изменения в Закон об информации, которыми установлен порядок ограничения доступа к информации, выражающей явное неуважение к обществу, государству, официальным государственным символам России, Конституции России или органам государственной власти. Процедура блокировки такой информации осуществляется Роскомнадзором аналогично вышеописанной процедуре, однако инициаторами процедуры также могут выступать Генеральный прокурор Российской Федерации или его заместители.

Особая процедура предусмотрена и для ограничения доступа к информации, распространяемой с нарушением авторских или смежных прав. В данном случае Роскомнадзор начинает процедуру ограничения доступа только после обращения правообладателя на основании вступившего в силу судебного акта (например, определения о принятии обеспечительных мер). В отношении исключительных прав на фильмы в сети “Интернет”, установлена специальная процедура защиты – Московский городской суд уполномочен принимать предварительные обеспечительные меры, направленные на обеспечение защиты исключительных прав на фильмы, и рассматривать дела, которые связаны с защитой исключительных прав на них.

Если же судом установлены факты неоднократного неправомерного размещения информации, содержащей объекты авторских или смежных прав, или информации, необходимой для их получения с использованием сети Интернет (например, торрент-трекеры), доступ к соответствующему сайту блокируется без возможности снятия ограничения, а на операторов поисковых систем возлагается обязанность прекратить выдачу сведений о соответствующем доменном имени и об указателях страниц сайта в сети Интернет. Копии (“зеркала”) заблокированных сайтов подлежат блокировке Роскомнадзором по обращению правообладателей и государственных органов.

11. Сотрудничество с иностранными партнерами

Патернализм и общая направленность на “импортозамещение” изменений, вносимых в российское законодательство в сфере ИТ за последние годы, все чаще заставляют иностранные компании задуматься о необходимости взаимодействия с российскими партнёрами с целью локализации соответствующей продукции (сервисов) в России. Такое сотрудничество может осуществляться как на договорной основе, так и путем создания совместных предприятий.

В последние годы гражданское законодательство России было дополнено многими положениями, знакомыми иностранным инвесторам и позволяющими урегулировать отношения сторон в рамках общепринятых правовых конструкций: например, корпоративные договоры (аналог Shareholders Agreement), опционы, заверения об обстоятельствах (Warranties & Representations), возмещение потерь (Indemnities) и т.п.

Таким образом, иностранный инвестор, находясь в российском правовом поле, может в полной мере обеспечить соблюдение своих интересов, даже являясь миноритарным участником проекта, и при необходимости выйти из проекта в соответствии с заранее согласованными сценариями.

12. Меры государственной поддержки ИТ-индустрии

Для компаний, осуществляющих деятельность в сфере информационных технологий, предусмотрены различные механизмы государственной поддержки.

Наиболее востребованными из них являются меры налогового стимулирования. В частности, при выполнении определенных условий относительно видов деятельности, выручки и персонала ИТ-компании возможно применение следующих видов льгот:

- снижение ставок страховых взносов на обязательное социальное, пенсионное и медицинское страхование (с общего максимального размера 30% до 14%);
- снижение налога на прибыль организаций за счет признания расходов на электронно-вычислительную технику.

Также действует ряд специальных льгот в отношении налога на добавленную стоимость (НДС):

- от НДС освобождается передача российской компанией исключительных прав на программное обеспечение и базы данных;
- с 01 июля 2019 года появляется возможность принять к вычету НДС по “экспортируемым” услугам или работам, в частности, по договорам на разработку программного обеспечения.

Для компаний, ориентированных на внешний рынок, будет интересным использование льгот, предусмотренных для резидентов особых экономических зон, с которыми успешно сочетаются другие виды налоговых преференций.

При выполнении определенных условий возможно использование упрощенной системы налогообложения ИТ-компаниями, что может быть актуально для упрощения отчетности в налоговые органы.

В качестве мер неналогового стимулирования можно рассматривать получение на конкурсной основе государственного софинансирования проектов российских ИТ-компаний. В частности, такая возможность предусмотрена в сфере разработки цифровых платформ и программных продуктов для производства высокотехнологичной промышленной продукции, а также для проектов компаний - лидеров по разработке продуктов, сервисов и платформенных решений на базе “сквозных” цифровых технологий (к которым, в частности, относятся: big data, нейротехнологии и искусственный интеллект, системы распределенного реестра, промышленный интернет, компоненты робототехники и сенсорики, технологии виртуальной и дополненной реальности). Условия участия в конкурсном отборе касаются, среди прочего, деятельности и опыта компании-соискателя, сроков реализации проектов и объемов затрат на их реализацию.

Авторы



Анна Афанасьева

Юрист | Партнер
БАЙТЕН БУРКХАРДТ Санкт-Петербург
Тел.: +7 812 4496000
Anna.Afanasyeva@bblaw.com



Сергей Богатырев

Юрист
БАЙТЕН БУРКХАРДТ Санкт-Петербург
Тел.: +7 812 4496000
Sergey.Bogatyrev@bblaw.com



Наталья Вильке

Юрист | Партнер
Глава Представительства
БАЙТЕН БУРКХАРДТ Санкт-Петербург
Тел.: +7 812 4496000
Natalia.Wilke@bblaw.com



БЕРЛИН | БРЮССЕЛЬ | ГАМБУРГ | ДЮССЕЛЬДОРФ | МОСКВА
МЮНХЕН | ПЕКИН | САНКТ-ПЕТЕРБУРГ | ФРАНКФУРТ-НА-МАЙНЕ

WWW.BEITENBURKHARDT.COM

06/2019