



ГРАЖДАНСКОЕ ПРАВО

CIVIL LAW

DOI: 10.22363/2313-2337-2020-24-4-985-1004

Научная статья

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ТАЙНЫ СВЯЗИ В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ

А.Н. Изотова

Национальный исследовательский университет «Высшая школа экономики»,
г. Москва, Российская Федерация

Освещается регулирование тайны связи, которая является не только гарантией индивидуального права на конфиденциальность, неприкосновенность частной жизни, но и необходимым условием коллективного блага — свободы слова, доверия к коммуникационным услугам, что имеет существенное значение для формирования информационного общества. Право на тайну связи с появлением новых коммуникационных технологий трансформируется и расширяется, что требует актуализации и гармонизации законодательной базы. В связи с этим *целью* исследования является выявление проблем и противоречий в обновляющемся правовом регулировании тайны связи, в том числе посредством анализа законодательства и существующих научных подходов по вопросам содержания тайны связи, раскрытия механизмов как обеспечения, так и ограничения тайны связи, а также взаимодействия субъектов правоотношений по поводу тайны связи. Также в работе затронуты вопросы соотношения российского и европейского законодательства, регулирующего вопросы тайны связи (ePrivacy). *Методология исследования* представлена такими методами, как диалектический, метод анализа, аналогии, формально-юридический, сравнительный методы научно-исследовательской деятельности. В исследовании в контексте взаимоотношений субъектов правоотношений по поводу тайны связи показаны различные подходы к определению содержания права на тайну связи, расширение круга профессиональных субъектов тайны связи, «расшатывание» механизмов ограничения данного права в сторону его расширения.

Ключевые слова: тайна переписки и телефонных переговоров, тайна связи, конфиденциальность, неприкосновенность частной жизни, электронные коммуникации, ограничение прав

Конфликт интересов. Автор заявляет об отсутствии конфликта интересов.

© Изотова А.Н., 2020.



This work is licensed under a Creative Commons Attribution 4.0 International License
<https://creativecommons.org/licenses/by/4.0>

Дата поступления в редакцию: 20 июня 2020 г.

Дата принятия к печати: 15 октября 2020 г.

Для цитирования:

Изотова А.Н. Правовое регулирование тайны связи в информационном обществе // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2020. Т. 24. № 4. С. 985–1004. DOI: 10.22363/2313-2337-2020-24-4-985-1004.

DOI: 10.22363/2313-2337-2020-24-4-985-1004

Research Article

LEGAL REGULATION OF COMMUNICATION PRIVACY IN THE INFORMATION SOCIETY

Anzhelika N. Izotova

National Research University Higher School of Economics,
Moscow, Russian Federation

Abstract. The article is devoted to the regulation of communication privacy, which is not only a guarantee of the individual right to confidentiality and privacy, but also a necessary condition for the collective freedom of speech, trust in communication services, which is essential for formation of the information society. The right to communication privacy with the advent of new communication technologies is being transformed and expanded, which requires updating and harmonization of the legal framework. In this regard, *the purpose* of the research is to reveal problems and contradictions in updating legal regulation of communication privacy, including by analyzing legislation and existent scientific approaches to the content of communication privacy, description of mechanisms for both ensuring and limiting communication privacy, as well as interaction of legal entities regarding communication privacy. The relationship between Russian and European legislation, which regulate communication privacy (ePrivacy) have been considered in this paper. *The research methodology* is represented by such methods as dialectical, analysis, analogies, formal-legal, comparative methods of research activity. The work demonstrates different approaches to determining the content of the right to communication privacy, expanding the range of professional subjects of communication privacy, and “loosening” the mechanisms for limiting this right in the direction of its expansion in the context of interrelations between subjects of legal relations concerning communication privacy.

Key words: ePrivacy, communication privacy, confidentiality, privacy, electronic communications, restriction of rights

Conflicts of interest. The author declared no conflicts of interest.

Article received 20 June 2020

Article accepted 15 October 2020

For citation:

Izotova, A.N. (2020) Legal regulation of communication privacy in the information society. *RUDN Journal of Law*. 24 (4), 985–1004. DOI: 10.22363/2313-2337-2020-24-4-985-1004.

Введение

Освоение новых технологий открыло новые горизонты для развития общества и права. Информатизация создала основу для приобретения информацией роли одного из важнейших ресурсов общества. Владение этим ресурсом может давать огромные возможности. Наряду с тем, что информация, информационные технологии, способы коммуникаций и возможности Интернета стали новой парадигмой существования и развития общества, возникло и множество проблем, связанных со способностью общества существовать в этой новой парадигме, среди которых можно выделить и проблему сохранения неприкосновенности частной жизни человека, а внутри нее и проблему тайны коммуникаций.

В данной статье рассматривается сложный характер понятия тайны связи, ее содержание и механизмы ограничения права на тайну связи, в том числе через взаимодействие субъектов правоотношений, возникающих по поводу тайны связи: пользователь — государство, поставщик услуг — абонент, которые становятся все более важными в коммуникационной среде. В работе большое внимание уделено судебной практике, поскольку в текущих условиях фактически содержание тайны связи формируется судами. Также затронуты вопросы соотношения российского и европейского законодательства, регулирующего вопросы тайны связи (ePrivacy) применительно к подходам об определении содержания тайны связи, принципов ограничения данного права, включая хранение данных, относящихся к тайне связи.

Понятие тайны связи

Конституция РФ в ч. 2 ст. 23 закрепила право каждого на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Сейчас ни у кого не вызывает сомнений эволюция тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений в тайну коммуникаций независимо от технических способов передачи информации. Дефиниция ч. 2 ст. 23 Конституции РФ приводит открытый перечень таких способов, говоря об «иных сообщениях». В Постановлении Пленума Верховного суда РФ № 46 от 25.12.2018 г. (п. 5) в качестве иных сообщений упомянуты любые сообщения, передаваемые по сетям электросвязи (включая электронные письма, мгновенные сообщения, видеозвонки).

Но если с традиционными средствами коммуникаций большая часть вопросов, касающихся регулирования тайны связи, стабилизировалась, то с *электронной почтой, мессенджерами и социальными сетями* ситуация неоднозначная.

В 2014 г. Федеральный закон «Об информации, информационных технологиях и защите информации» от 27.07.2006 г. № 149-ФЗ дополнен статьей 10.1,

регулирующей деятельность организаторов распространения информации в сети «Интернет»¹.

Законодатель выделил специальную категорию организаторов распространения информации в сети «Интернет» — организаторов сервиса обмена мгновенными сообщениями, квалифицирующим признаком которых является использование информационных систем и программного обеспечения для обмена электронными сообщениями между их пользователями, при этом не предусматриваются размещение пользователями общедоступной информации, а также передача электронных сообщений неопределенному кругу лиц. Таким образом, под определение организатора сервиса обмена мгновенными сообщениями попали социальные сети, мессенджеры. Сервисы электронной почты не имеют указанного признака (т.к. обмен электронными сообщениями возможен с пользователями и других сервисов) и поэтому относятся к «обычным» организаторам распространения информации в сети «Интернет».

Данное разграничение организаторов распространения информации в сети «Интернет» важно отметить, поскольку для организатора сервиса это влечет разный объем обязанностей. Интересно, что только для организатора сервиса обмена мгновенными сообщениями в статье 10.1 Федерального закона «Об информации» закреплена обязанность обеспечивать конфиденциальность передаваемых электронных сообщений. Вспомним, что согласно пунктам 4, 5 статьи 9 названного закона в качестве условия отнесения информации к тайнам, в том числе профессиональной тайне, названо прямое указание на это в федеральном законе, поэтому вырисовывается странная картина: организатор распространения информации в сети «Интернет», не являющийся организатором сервиса обмена мгновенными сообщениями, не ограничен профессиональной тайной в части электронных сообщений пользователей. Такой подход законодателя представляется непоследовательным. Регулирование правоотношений, складывающееся по поводу передачи электронных сообщений, поставлено в зависимость от субъекта, обеспечивающего такую передачу. Вместе с тем по своей сути они идентичны отношениям по передаче сообщений операторами связи по сетям электросвязи. На наш взгляд, это создает предпосылки для схожего правового регулирования деятельности организаторов распространения информации в сети «Интернет», которые организуют обмен электронными сообщениями.

Следует отметить, что европейское законодательство страдает тем же недостатком, защищая сведения, относящиеся к тайне коммуникаций, лишь применительно к оказанию общедоступных услуг связи. Директива № 2002/58/ЕС

¹ Под организатором распространения информации в сети «Интернет» понимается 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 отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи (Директива о конфиденциальности и электронных средствах связи)»² (далее — Директива ePrivacy) не распространяется на охрану коммуникаций в коммуникационных сервисах, отличных от услуг операторов связи. Причем ограниченный характер регулирования отмечался учеными сразу после принятия Директивы (Papakonstantinou, Hert, 2011). Дискуссии в обществе привели к появлению проекта Регламента Европейского парламента и Совета Европейского Союза в отношении уважения частной жизни и защиты персональных данных в секторе электронных средств связи взамен Директивы 2002/58/ЕС³, который призван в том числе распространить защиту на все коммуникационные сервисы, формируя максимально широкий и технологически нейтральный подход к тайне связи. Пока этот проект проходит обсуждение.

Применительно к деятельности по передаче электронных сообщений организаторами распространения информации в сети «Интернет» в законодательстве отсутствует какое-либо упоминание о тайне связи. Но анализ судебной практики показывает, что в силу прямого действия Конституции России суды распространяют режим тайны связи на электронные сообщения, передаваемые организаторами распространения информации в сети «Интернет», когда речь не идет о передаче сообщений неопределенному кругу лиц⁴. То есть судебная практика в таких случаях восполняет пробелы в правовом регулировании.

Итак, субъектами, обеспечивающими тайну связи, являются операторы связи, операторы почтовой связи и организаторы распространения информации в сети «Интернет» в части обмена электронными сообщениями между пользователями (исключая размещение общедоступной информации в сети «Интернет» и коммуникации с неопределенным кругом лиц). Законодательство в данной части требует определенной гармонизации для эффективной защиты сведений, составляющих тайну связи.

В законодательстве России не содержится формализованного определения тайны связи либо критериев, которые позволили бы определить ее границы, что приводит к различному толкованию содержания тайны связи. Важную роль в преодолении подобной ситуации также играет судебная практика.

² Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02002L0058-20091219> (Accessed 20 May 2020).

³ Proposal for a regulation of the European parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC: Regulation on Privacy and Electronic Communications, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:0010:FIN> (Accessed 30 May 2020).

⁴ Постановление Конституционного суда РФ от 26.10.2017 г. № 25-П // Справочная правовая система «КонсультантПлюс».

Конституционный суд РФ в Определениях № 345-О от 02.10.2003 г. и от 21.10.2008 № 528-О-О высказал позицию, что к тайне связи относятся любые сведения, передаваемые, сохраняемые и устанавливаемые с помощью телефонной аппаратуры, включая данные о входящих и исходящих сигналах соединений телефонных аппаратов конкретных пользователей, то есть *как содержание соединений, так и информация о соединениях*.

Указанный «широкий» подход доминирует в российской доктрине. Вместе с тем, ввиду расширительного толкования тайны связи, такой подход подвергается критике со стороны отдельных ученых. Так, А. Чететин (Chechetin, 2005:40) и А. Богдановский (Bogdanovskii, 2006:34) в своих работах резко высказывались о необоснованном распространении режима тайны связи на сведения о соединениях, полагая, что Конституционный суд ошибочно истолковал положения ст. 63 Федерального закона «О связи» и его аргументы «противоречат Конституции РФ, другому действующему законодательству и здравому смыслу». А. Рего и А. Мацкевич также ставят под сомнение целесообразность отнесения технических идентификаторов абонентского оборудования к тайне связи, основывая свою позицию на существенно меньшей ценности такой информации для абонента в сравнении с содержанием коммуникаций (Rego, Matskevich, 2019:18).

Вместе с тем данная точка зрения идет в разрез с тенденциями расширения содержания тайны связи. Как ранее было отмечено, законодатель и суды (как российские, так и европейские, а также других стран мира) идут по пути применения норм о тайне связи не только к отношениям, связанным с услугами связи, но и к отношениям, складывающимся по поводу использования других коммуникационных сервисов, что способствует повышению доверия к таким сервисам и отвечает потребностям информационного общества. Кроме того, нельзя согласиться с аргументами о меньшей ценности сведений о сообщениях по сравнению с содержанием сообщений. Отдельные данные о сообщениях, особенно их совокупность, позволяют составить очень точную, детальную картину о человеке и его личной идентичности (Hoboken, Zuiderveen Borgesius, 2015).

Длительное время судебная и правоприменительная практика складывалась достаточно единообразно в соответствии с приведенной позицией Конституционного суда. Однако на протяжении последних лет отмечается активная деятельность государственных органов по запросу сведений о соединениях (IP-адресов, IMEI). Во многих случаях это объясняется попыткой изменить подход к праву отдельных государственных органов на доступ к тайне связи, что будет рассмотрено в следующем разделе статьи. Тем не менее, в части дел, касающихся предоставления собственно сведений о соединениях, судебная практика устояла на позиции, что такие сведения относятся к тайне связи⁵.

⁵ Пункт 11 Постановления Пленума Верховного суда РФ от 01.06.2017 г. № 19, пункт 4 Постановления Пленума Верховного суда РФ от 25.12.2018 г. № 46 // Справочная правовая система «КонсультантПлюс».

Широкий подход к тайне связи применяется и в праве Европы, где сильна концепция прав человека. Директива e-Privacy устанавливает защиту сведений о соединениях и данных о местоположении пользователей (метаданных). Суды Европы отмечают не меньшую ценность метаданных, чем содержания сообщений с точки зрения неприкосновенности частной жизни (Zuiderveen Borgesius, Steenbruggen, 2018).

Следует обратить внимание на ряд судебных решений относительно *сведений об абонентах, которым выделялся конкретный IP-адрес в конкретные даты и время и осуществивших выход на определенный интернет-ресурс*. Если ранее суды⁶ относили сведения об абонентах в рамках запросов таких сведений государственными органами к тайне связи, то впоследствии их позиция изменилась, такие сведения стали квалифицироваться как персональные данные абонента⁷. Выводы судов сводятся к тому, что информация о пользователях услугами связи не относится к тайне связи, поскольку государственным органом запрашивались лишь сведения об абоненте, совершившем соединение, а не данные о самом соединении. То есть судебная практика пошла по пути, когда данные об абоненте, определенные на основании сведений об IP-адресе, с которого был совершен выход на конкретный интернет-ресурс в определенный промежуток времени, относятся к сведениям об абоненте, как это определено в ст. 53 Федерального закона «О связи», и на них не распространяется жесткий режим защиты тайны связи.

В судебных постановлениях не случайно упоминается именно динамический IP-адрес, который присваивается абоненту на время конкретного соединения (в отличие от статического, который закрепляется за абонентом в абонентском договоре об оказании услуг связи). Следуя логике судов, оператор связи, получив от государственного органа (зачастую запросы поступают от Федеральной антимонопольной службы (ФАС)) запрос с указанием динамического IP-адреса, посещенного сайта, времени его посещения, должен обратиться к своим системам, найти данное соединение по времени и IP-адресу, «открыть» содержание соединения (установить ресурс, к которому обращался абонент) и соотнести эти данные с данными об абоненте, имеющимися в базе оператора. Такая позиция судов означает, что оператор связи для ответа на запрос государственного органа вправе получить доступ к соединениям абонента, которые являются тайной связи, что противоречит общему подходу о доступе к тайне связи только по решению суда.

Необходимо отметить, что приведенные примеры касаются судебных дел, где вопрос касается исключительно предоставления сведений об абонен-

⁶ Определение Московского городского суда от 06.03.2012 г. № 33-7194 // Справочная правовая система «КонсультантПлюс».

⁷ Постановление Верховного суда РФ от 30.03.2016 г. № 82-АД16-1 // Справочная правовая система «КонсультантПлюс».

тах. Если же запрос содержит требование о предоставлении сведений об абоненте и сведений о соединениях, суды разделяют указанные в запросе требования и признают требования о предоставлении сведений о соединениях незаконными и необоснованными⁸. Однако, если обратиться к судебной практике по делам, не связанным напрямую с тайной связи (в основном это дела о нарушении законодательства о рекламе и распространении спама), их анализ показывает, что суды придерживаются позиции, что операторы связи не имеют права доступа к сведениям, составляющим тайну связи, а являются лишь «трубой», по которой идут сигналы электросвязи. Примечательно, что ФАС в судебных спорах о нарушении законодательства о рекламе отказывается предоставлять полученные от интернет-провайдера сведения об абоненте в отношении конкретного соединения, ссылаясь именно на нормы о тайне связи⁹. Поэтому пока рано ставить точку в споре о правовом режиме информации в указанных выше спорах.

Ограничение права на тайну связи

Отношение государства к тайне коммуникации, доступность этой информации для государства в лице его органов напрямую влияет на то, насколько человек доверяет власти, открыт для нее и готов сотрудничать в вопросах как личного, так и социального характера. Для того, чтобы обеспечить такое доверие и сотрудничество, необходимо гарантировать конфиденциальность данных человека вообще и его коммуникаций в частности и создать условия и правила регулирования, исключающие возможность манипулирования сведениями, содержащими тайну связи.

В ч. 3 ст. 55 Конституции России сформулировано общее основание ограничения прав человека федеральным законом только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Современная доктрина, а также судебная практика при ограничении конституционных прав исходят из обязательного соблюдения принципа соразмерности ограничений прав (Barak, 2012; Vendor, Sela, 2015:530–544), контекстуального и целевого характера применяемых ограничений.

Указанные принципы повторяют европейский подход, согласно которому ограничение права на тайну коммуникаций должно преследовать законную цель, быть необходимым и соразмерным этой цели. ЕСПЧ считает такие принципы необходимыми в демократическом обществе, и государственные органы

⁸ Постановление Верховного суда РФ от 11.10.2016 г. № 82-АД16-5 // Справочная правовая система «КонсультантПлюс».

⁹ Решение УФАС по Ульяновской области от 16.05.2016 г. № 11784/06-2015 // Справочная правовая система «КонсультантПлюс».

должны предоставить соответствующие и достаточные обоснования для установления ограничений (Brunner, 2018: 217–242).

Для ограничения права на тайну связи также необходимо соответствующее судебное решение. Так, законодатель стремился обеспечить баланс между свободой и безопасностью — двумя конфликтующими конституционными ценностями. А. Соболева высказала мнение, что вмешательство государства в личную жизнь допустимо постольку, поскольку это оправданно в каждом конкретном случае, с соблюдением специальной процедуры (Dedov, Jakushev, Belov, Golovko, et al., 2018:26). Нарушение баланса безопасности и свободы чревато существенными негативными последствиями. Как отмечал Н.С. Бондарь, «государство, не обеспечивающее последовательную защиту свободы, рискует превратиться в тоталитарный режим» (Bondar', 2005:30–31).

Нельзя не упомянуть Постановление ЕСПЧ по делу «Роман Захаров против России» от 04.12.2005 г., где суд установил нарушение прав заявителя ввиду недостаточного контроля за доступом к тайне коммуникаций и отметил, что основания ограничения права на тайну переписки должны быть достаточно определенными с точки зрения толкования.

Ограничение тайны связи можно представить моделями *ex-ante* («предварительный контроль») и *ex-post* («итоговый контроль»). К модели *ex-ante* относятся введенные так называемым «законом Яровой»¹⁰ обязательства по фиксации и хранению информации о пользователях и о совершенных ими соединениях, а также содержания таких соединений операторами связи и организаторами сервисов распространения информации в сети «Интернет». Модель *ex-post* основана на доступе уполномоченных государственных органов в случаях, установленных законодательством, к сведениям, имеющимся у операторов связи и организаторов распространения информации в сети «Интернет».

Федеральный закон «Об оперативно-розыскной деятельности»¹¹ предписывает органам, осуществляющим оперативно-розыскную деятельность (органам ОРД), проведение оперативно-розыскных мероприятий (ОРМ), которые ограничивают право на тайну коммуникаций, на основании судебного решения и только в случаях, предусмотренных законом.

В отдельных случаях проведение ОРМ допускается без судебного решения, а точнее с отсрочкой его получения. Так, согласно ст. 8 Федерального закона «Об ОРД» возможно проведение ОРМ на основании мотивированного постановления руководителя органа ОРД с обязательным уведомлением суда в течение 24 часов в случаях, не терпящих отлагательства и способных приве-

¹⁰ Федеральный закон от 06.07.2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон “О противодействии терроризму” и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // Справочная правовая система «КонсультантПлюс».

¹¹ Федеральный закон «Об оперативно-розыскной деятельности» от 12.08.1995 г. № 144-ФЗ // Справочная правовая система «КонсультантПлюс».

сти к совершению преступления, а также при угрозе государственной, военной, экономической, информационной или экологической безопасности. При этом обязанность получения судебного решения в течение 48 часов с момента начала проведения ОРМ сохраняется, в противном случае проведение ОРМ надлежит прекратить. Подобный механизм предусмотрен и в случае сообщения о без вести пропавшем несовершеннолетнем с согласия одного из его родителей или лиц, их заменяющих. Хотя принятию данной нормы в августе 2019 г. предшествовали длительные обсуждения, в том числе и в научной литературе (Gushev, Shuvalova, 2015:65).

В дополнение к положениям о хранении данных о соединениях в постановление Правительства РФ от 27.08.2005 г. № 538 «Об утверждении правила взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность» внесены изменения, устанавливающие возможность круглосуточного доступа органов Федеральной службы безопасности (ФСБ) к хранилищу и базе данных операторов связи — между системой оператора связи и пультом управления органа ФСБ должен быть налажен постоянный канал связи.

Правила хранения информации об электронных сообщениях пользователей, а также порядок предоставления такой информации уполномоченным государственным органам организаторами распространения информации в сети «Интернет» урегулирован Постановлением Правительства РФ от 31.07.2014 г. № 759. Данным постановлением также предусмотрен круглосуточный удаленный доступ уполномоченных органов к информационной системе организатора распространения информации в сети «Интернет».

Исполнение «закона Яровой» у многих вызвало опасения ввиду возможного нарушения прав граждан на тайну связи. Нарушение конституционных положений связано с реализацией указанного постановления Правительства РФ о доступе органов ФСБ к базам данных операторов связи, что открывает широкие возможности для злоупотреблений. Однако Верховный суд РФ в апелляционном определении от 05.03.2019 г. № АПЛ 19-53 признал Постановление Правительства РФ № 538 законным и указал, что в нем лишь закреплен порядок взаимодействия между операторами связи и органами, осуществляющими ОРД, но не отменена необходимость получения судебного решения.

Следует отметить, что идея хранения данных, составляющих тайну связи, заимствована Россией в Европе, где была принята Директива 2006/24/ЕС о хранении данных¹², обязывавшая операторов связи хранить значительный перечень данных, относящихся к тайне связи. Тем не менее, в 2014 г. Европей-

¹² Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32006L0024> (Accessed 02 April 2020).

ским судом было вынесено решение о недействительности Директивы, поскольку реализация ее положений приводила к серьезному вмешательству в тайну коммуникаций и неприкосновенность частной жизни в целом. Суд ЕС также установил, что вмешательство в тайну коммуникаций несоизмеримо целям Директивы. Однако в научном сообществе считают, что хранение данных об электронных сообщениях может иметь место, но правовое регулирование должно, помимо основной цели обеспечения безопасности государства, гарантировать неприкосновенность частной жизни (Drewry, 2016).

В отношении ограничения права на тайну связи при проведении ОРМ и противодействию терроризму алгоритм взаимодействия между операторами связи, организаторами распространения информации в сети «Интернет» и органами ОРД налажен, судебная практика представляется достаточно сформированной (Tereshhenko, 2016:151), хотя и встречаются случаи, когда получение сведений, относящихся к тайне связи, происходило без судебного решения¹³.

Кроме органов ОРД, на получение сведений, составляющих тайну связи, претендуют и другие органы исполнительной власти. Особенной активностью отличается ФАС, о чем свидетельствует обширная судебная практика об обжаловании решений ФАС о привлечении операторов связи к административной ответственности за отказ в предоставлении сведений, относящихся к тайне связи.

ФАС мотивирует свое право на доступ к тайне связи статьей 34 Федерального закона от 13.03.2006 г. № 38-ФЗ «О рекламе», из которой следует обязанность юридических лиц и индивидуальных предпринимателей предоставлять ФАС необходимую информацию, в том числе составляющую охраняемую законом тайну. Однако Верховный суд РФ не поддержал ФАС в его притязаниях на получение информации, относящейся к тайне связи, сославшись на ст. 53 Федерального закона «О связи», в соответствии с которой сведения об оказанных абонентам услугах связи могут быть предоставлены только в установленных законом случаях¹⁴. Вместе с тем ст. 64 Федерального закона «О связи» предоставляет право получения сведений об абонентах и оказанных им услугах лишь органам ОРД, к которым ФАС не относится.

В связи с распространением электронных коммуникаций, совершением все большего числа правонарушений в цифровой среде антимонопольной службе все чаще требуются сведения о соединениях пользователей услугами связи. Кроме регулирования рынка рекламы, ФАС является государственным органом, осуществляющим надзор в сфере защиты конкуренции, а «реализация программы “Цифровая экономика” ставит новые задачи при выявлении сговоров на торгах, которые трудно решить в рамках действующего регулирования тайны

¹³ Апелляционное определение Иркутского областного суда от 06.08.2015 г. № 33-6970/2015 // Справочная правовая система «КонсультантПлюс».

¹⁴ Постановление Верховного суда РФ от 04.03.2016 г. № 307-АД15-18844 // Справочная правовая система «КонсультантПлюс».

связи» (Tenishev, 2018:18). Все это приводит к появлению различных предложений по изменению подхода к тайне связи и доступа к ней антимонопольной службы. Среди них проект федерального закона, инициированный ФАС, о внесении изменений в законодательство о защите конкуренции¹⁵. Целью этого законопроекта, как отмечают его инициаторы, является лишь отграничение информации о пользователях услугами связи от информации, подпадающей под правовой режим тайны связи. С моей точки зрения, данный законопроект направлен на выведение сведений о соединениях из-под жесткого регулирования тайны связи. Более рациональным и оправданным представляется предложение о наделении ФАС правом запрашивать информацию, составляющую тайну связи, на основании судебного решения и регламентации порядка предоставления таких сведений, как это предусмотрено для органов ОРД (Rego, Matskevich, 2019:18).

Судебная практика знает примеры запросов сведений, относящихся к тайне связи, и иными органами власти. Так, Верховный суд РФ признал запрос территориального Управления Федеральной службы судебных приставов незаконным, основываясь на том, что ограничение права на тайну связи допускается только на основании судебного решения и исключительно при осуществлении органами ОРД своих полномочий¹⁶.

Подобная практика существует и в отношении Центрального банка России¹⁷. При этом нельзя не отметить, что законодатель предоставил Центральному банку право запрашивать сведения, относящиеся к тайне связи, лишь в части информации о почтовых денежных переводах, и если они необходимы для осуществления Банком России его полномочий в отношении неправомерного использования инсайдерской информации и манипулирования рынком¹⁸.

Как было указано выше применительно к ФАС, в условиях развития цифровых сервисов, data-технологий появляются законодательные инициативы, связанные с расширением возможностей доступа государственных органов к сведениям, относящимся к тайне связи. Среди них можно также назвать разработанный Министерством экономического развития РФ законопроект «О вне-

¹⁵ Проект федерального закона «О внесении изменений в Федеральный закон “О защите конкуренции” и отдельные законодательные акты Российской Федерации в части повышения эффективности выявления и пресечения ограничивающих конкуренцию соглашений и согласованных действий», available at: <https://sozd.duma.gov.ru/bill/848392-7> (Accessed 07 June 2020).

¹⁶ Определение Верховного суда РФ от 14.11.2018 г. № 308-КГ18-8447 // Справочная правовая система «КонсультантПлюс».

¹⁷ Постановление Федерального арбитражного суда Московской области от 12.03.2014 г. по делу № А40-56142/13-130-551, Постановление Девятого арбитражного апелляционного суда от 05.05.2014 г. № 09АП-8322/2014 // Справочная правовая система «КонсультантПлюс».

¹⁸ Федеральный закон от 27.07.2010 г. № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» // Справочная правовая система «КонсультантПлюс».

сении изменений в статью 63 Федерального закона «О связи»¹⁹, целью которого указана выработка подхода, учитывающего основные права человека и интересы инновационного бизнеса, возникшие как результат научно-технического прогресса. Законопроект предусматривает возможность операторов связи обрабатывать сведения о соединениях в целях исполнения договора об оказании услуг связи, а также предоставлять отдельные сведения о сообщениях (дата и время оказания услуги связи, продолжительность телефонных переговоров, абонентские номера абонентов, уникальные коды идентификации абонентов (метаданные)) уполномоченным органам в случаях, установленных федеральными законами. Указанные действия, по предложению инициатора законопроекта, не должны считаться нарушением тайны связи.

Это свидетельствует либо о сужении содержания тайны связи путем исключения из него сведений о соединениях (сообщениях) с последующим предоставлением сведений как персональных данных субъекта соответствующим государственным органам, либо о том, что цели ограничения права на тайну связи, предусмотренные ст. 55 Конституции РФ, предлагается расширить целями развития экономики и научно-технического прогресса, что представляется чрезмерным и нарушающим основные гарантии права на тайну связи. На данный момент ни то, ни другое обоснование не представляется убедительным для принятия данного законопроекта.

Следует отдельно остановиться на вопросе о возможности *ограничения тайны связи с согласия лица*, которому оно принадлежит. Одним из правомочий в составе неприкосновенности частной жизни является контроль человека над его данными, включая сведения, охраняемые режимом тайны связи (Post, 2017). Формулировка п. 4 ст. 63 Федерального закона «О связи» свидетельствует о возможности предоставления сведений о сообщениях отправителям и получателям, а также их уполномоченным представителям. Представительство по своей правовой природе является одной из форм посредничества, делегированием права одним лицом другому лицу осуществлять деятельность в интересах первого и представлять его интересы перед третьими лицами (Nevzgodina, 2012:126). В данном контексте полагаю, что согласие может рассматриваться как частный случай представительства в смысле уполномочивания другого лица (в том числе государственного органа) на получение сведений, составляющих тайну связи.

Среди законодательных примеров «разрешительного» ограничения права может быть приведена ст. 9 Федерального закона «Об ОРД», в которой разрешается прослушивание телефонных переговоров в случае возникновения угрозы жизни, здоровью, собственности отдельных лиц с их согласия на осно-

¹⁹ Проект Федерального закона «О внесении изменений в статью 63 Федерального закона «О связи», available at: <https://regulation.gov.ru/projects#npa=94552> (Accessed 01 June 2020).

вании соответствующего постановления органа ОРД с обязательным уведомлением суда.

Подобную практику переняла и ФАС, указывая, что антимонопольному органу для проведения проверки по жалобе абонента по нежелательным сообщениям требуется согласие абонента на получение необходимых сведений от оператора связи, оказывающего абоненту услуги связи²⁰. Схожий подход применяется и в отношении других видов тайн (тайны частной жизни, врачебной тайны).

Как отмечает все больше авторов, «развитие цифровой экономики, возможно, потребует пересмотра принципов защиты различных видов тайны», в том числе тайны связи, обуславливая это назревшей необходимостью изменения порядка передачи сведений, составляющих различные виды тайн, с согласия профессиональных субъектов третьим лицам для достижения государственных, социально-экономических целей (Vairan, Egorova, (eds.), 2019:376).

Поставщик коммуникационных услуг и абонент (пользователь)

С либерализацией и приватизацией собственность на информационную инфраструктуру перешла к частным лицам, которые сейчас в большинстве случаев оказывают информационные услуги. Защита интересов пользователей и гарантии их прав на тайну коммуникаций, а также контроль коммерческих интересов поставщиков услуг по использованию и злоупотреблению этими данными стали важным компонентом современной конфиденциальности связи.

Одним из базовых и основных условий соблюдения права на тайну коммуникаций является *защита инфраструктуры*, которая используется для обеспечения деятельности по обработке информации, являющейся тайной связи.

Законодательство РФ отводит серьезную роль мерам, которые должны быть реализованы для того, чтобы операторы связи обеспечили гарантии по соблюдению тайны связи, указывая на то, что сети и сооружения связи находятся под защитой государства. Федеральным законом «О связи» (п.п. 2, 3 ст. 7, ст. 41) на операторов возложена обязанность по защите сетей и сооружений связи, а также соблюдению требований о подтверждении соответствия средств и услуг связи в виде обязательной сертификации или декларирования.

В отношении защиты информации, передаваемой организаторами распространения информации в сети «Интернет», отсутствует такое детальное регулирование защиты информации, как для операторов связи. Статья 10.1 Федерального закона «Об информации» довольно сухо предписывает лишь организаторам сервиса обмена мгновенными сообщениями обеспечивать конфиденци-

²⁰ Письмо ФАС РФ от 11.11.2019 № ДФ/98054/19 «О надлежащих доказательствах при выявлении нарушения требований части 1 статьи 18 Федерального закона “О рекламе”» // Справочная правовая система «КонсультантПлюс».

альность передаваемых электронных сообщений (пп. 4 п. 4.2). Конечно, при оказании сервисов обмена электронными сообщениями используются те же сети связи, защиту которых обеспечивает оператор связи при оказании услуг связи. Вместе с тем представляется, что обязанность обеспечения конфиденциальности электронных сообщений должна быть возложена на всех организаторов распространения информации в сети «Интернет», предоставляющих услуги по передаче электронных сообщений (не считая передачу сообщений неопределенному кругу лиц).

С введением «законом Яровой» появились обязанности операторов связи хранить информацию о сообщениях, а также сами сообщения, появились и нормы об обязательной сертификации оборудования, необходимого для хранения данных. Однако проблема исполнения требований закона заключается в отсутствии лабораторий, которые могут осуществлять сертификацию средств накопления данных; не приняты нормативные акты, регулирующие порядок такой сертификации. Таким образом, данный пробел в законодательстве формально служит причиной того, что операторы связи и сервис-провайдеры не могут выполнять требования закона о хранении данных. В связи с этим появляются разъяснения региональных органов ФСБ как органа, уполномоченного осуществлять надзор за выполнением требований «закона Яровой», позволяющие операторам связи и сервис-провайдерам использовать декларируемые производителем технические средства накопления информации при условии их обязательной сертификации в течение 3 месяцев с после появления сертифицирующих лабораторий²¹. Вместе с тем правовая сила таких разъяснений вызывает сомнения уже ввиду того, что законом установлены обязательные требования по сертификации оборудования, необходимого для хранения данных, также за использование операторами связи несертифицированного оборудования Кодексом об административных правонарушениях РФ (п. 1 ст. 13.6) предусмотрена ответственность в виде штрафа с конфискацией несертифицированного оборудования.

Несмотря на неоднозначность ситуации, в РФ уже появилась судебная практика, которая устанавливает обязанность операторов использовать несертифицированное оборудование, согласовав его применение с органами ФСБ²².

Вторым условием обеспечения тайны связи является *идентификация абонентов/пользователей* услугами связи, сервисов обмена электронными сообщениями.

Идентификация абонентов операторами связи носит комплексный характер и включает собственно идентификацию при заключении договора, проверку достоверности сведений об абоненте, а также обеспечение актуальности сведений об абоненте на протяжении всего периода обслуживания.

²¹ Галушко Д. (2018) Яровая + COPM: правила вступили в силу. Что дальше? Available at: <https://nag.ru/articles/article/102832/yarova-ya-sorm-pravila-vstupili-v-silu-cto-dalshe-.html> (Accessed 29 May 2020).

²² Постановление Пятнадцатого Арбитражного апелляционного суда от 12.12.2019 г. № 15АП-20381/2019, available at: <https://kad.arbitr.ru/Card/54516754-7ba1-413a-a162-16d7b4c79e66> (Accessed 25 May 2020).

Федеральный закон «О связи» (ст. 44) закрепляет порядок заключения договоров об оказании услуг связи как самим оператором связи, так и уполномоченным им лицом, при личном присутствии абонента либо посредством сети «Интернет» с использованием электронной подписи.

Процедура проверки достоверности предоставленных абонентом сведений о его имени, дате рождения, данных документа, удостоверяющего личность, обеспечивается проверкой оригинала документа, удостоверяющего личность, а также дистанционными способами проверки, установленными законом. Данная процедура распространяется и на пользователей абонентов — юридических лиц (за рядом исключений). Дистанционные способы проверки достоверности легализованы с июля 2018 года и постепенно начинают применяться операторами связи, что, с одной стороны, позволяет расширить возможности дистанционного подключения услуг связи, а с другой — обеспечивает идентификацию абонентов/пользователей такими услугами.

Законодательство в области регулирования отношений в социальных сетях и мессенджерах также идет в направлении деанонимизации пользователей (Kufleva, Kubrak, 2018:15). Применительно к организаторам распространения информации в сети «Интернет» идентификация пользователей сервиса вменена в качестве обязанности лишь российским организаторам сервиса обмена мгновенными сообщениями и сведена к установлению абонентского номера подвижной связи пользователя сервиса²³. Отсутствие обязательной идентификации для пользователей иных сервисов распространения информации в сети «Интернет», отличных от сервисов обмена мгновенными сообщениями, но осуществляющих такую же деятельность по обмену электронными сообщениями, может приводить к спорным ситуациям. В частности, суд указал на отсутствие тайны связи в коммуникациях посредством сервиса электронной почты Рамблер на том основании, что при создании ящика электронной почты пользователь может не указывать свои персональные данные²⁴.

Идентификация необходима для обеспечения тайны связи и исключения доступа к ней третьих лиц не только при заключении договора, но и при обслуживании абонентов (пользователей) в процессе его исполнения. В том числе и для этих целей операторы связи обязаны обеспечивать актуальность информации об абонентах и оказанных им услугах в своих базах (п. 12 постановления Правительства РФ от 27.08.2005 г. № 538).

Взаимосвязь поставщика услуг и пользователя коммуникационными услугами также состоит в *доступности таких сведений для самого поставщи-*

²³ Постановлением Правительства РФ «Об утверждении Правил идентификации пользователей информационно-телекоммуникационной сети «Интернет» организатором сервиса обмена мгновенными сообщениями» от 27.10.2018 № 1279 // Справочная правовая система «КонсультантПлюс».

²⁴ Постановление Девятого арбитражного апелляционного суда от 19.09.2013 г. № 09АП-29641/2013 // Справочная правовая система «КонсультантПлюс».

ка услуг. Как следует из п. 3 ст. 63 Федерального закона «О связи», доступ к сведениям, относящимся к тайне связи, имеют только отдельные уполномоченные сотрудники оператора связи в целях исполнения договора об оказании услуг связи.

Интересным с точки зрения отношений пользователя и поставщика услуг является спор между ООО «Гугл» и пользователем электронной почты, который обнаружил, что демонстрируемая ему в сервисе электронной почты реклама соответствует содержанию его электронной переписки. В результате рассмотрения спора судебная коллегия пришла к выводу, что ООО «Гугл», размещая рекламу в сообщениях пользователя, руководствовался результатами мониторинга электронной корреспонденции пользователя, чем нарушил тайну его переписки²⁵.

Еще одним показательным примером вмешательства оператора связи в тайну связи его абонента является дело в отношении ОАО «МГТС»²⁶ о передаче рекламному агентству сведений об оказанных абонентам телематических услугах связи (сведений о посещаемых интернет-страницах, IP-адресах, о поисковых запросах и пр.) для формирования профиля абонента и последующего направления рекламы (Soldatova, 2020:38). Вместе с тем представляется сомнительным, что вмененное ОАО «МГТС» правонарушение было рассмотрено с точки зрения разглашения персональных данных абонентов, но не рассматривалось судом как нарушение их тайны связи.

Таким образом, взаимодействие поставщиков коммуникационных услуг с пользователями услуг складывается в двух основных направлениях: защита сведений, составляющих тайну связи, путем защиты коммуникационной инфраструктуры, предоставления доступа к информации, составляющей тайну связи, только пользователям таких услуг и сервисов после их идентификации, и ограничение доступа к таким сведениям самого оператора (его сотрудников).

Заключение

Право на тайну связи является одним из основных прав в современном информационном обществе. Несмотря на это, объем тайны связи законодательно не закреплен, что вызывает множество споров по этому поводу. Более того, технологии передачи информации развиваются, что еще больше увеличивает число спорных вопросов. Фактически содержание тайны связи сейчас определено судебной практикой и в него входит как содержание соединений, так и сведения о них. Вместе с тем появляется все больше сторонников узкого подхода к тайне связи, выступающих за то, что собственно тайну связи составляет

²⁵ Апелляционное определение Московского городского суда от 16.09.2015 г. по делу № 33-30344 // Справочная правовая система «КонсультантПлюс».

²⁶ Постановление Девятого арбитражного апелляционного суда от 23.05.2016 г. № 09АП-17574/2016 // Справочная правовая система «КонсультантПлюс».

лишь содержание соединений. В том числе это объясняется необходимостью преодоления существующих законодательных барьеров для развития инноваций, data-технологий и цифровых сервисов.

Тайна связи является многогранным институтом с точки зрения отношений между разными субъектами. Кроме традиционных субъектов, обеспечивающих тайну связи как профессиональную тайну, к которым можно отнести операторов связи, с развитием информационных технологий и коммуникационных услуг свое место в правоотношениях, возникающих по поводу тайны связи, заняли организаторы распространения информации в сети «Интернет». Вместе с тем различие в подходах законодателя к обязанностям таких субъектов по защите тайны связи по сравнению с операторами связи, а также между организаторами сервисов обмена мгновенных сообщений и другими организаторами распространения информации в сети «Интернет» представляется спорным и требует унификации.

Тайна связи как конституционное право может быть ограничена. Как правило, такое ограничение происходит со стороны государства. Однако любое ограничение должно осуществляться в соответствии с законом, с законной целью и быть необходимым и соразмерным. Ограничение права на тайну связи допустимо на основании судебного решения и только теми государственными органами, чьи полномочия позволяют получать доступ к сведениям, составляющим тайну связи. Вместе с тем при соблюдении установленных Конституцией России условий ограничения права на тайну связи, издании соответствующих федеральных законов возможно расширение круга субъектов, имеющих доступ к тайне связи.

Большое количество спорных моментов в правовом регулировании тайны связи требует детальной проработки как на уровне теоретических подходов, так и в контексте практических интересов всех сторон правоотношений. И все это нам еще предстоит решить, чтобы построить если не «светлое будущее», то хотя бы нормально функционирующее цифровое общество.

Библиографический список / References

- Barak, A. (2012) *Proportionality. Constitutional Rights and their Limitations*. Proportionality. Constitutional Rights and their Limitations. Cambridge University Press, available at: <https://doi.org/10.1093/icon/mov028>
- Bendor, A. L. Sela, T., (2015) How proportional is proportionality? *International Journal of Constitutional Law*. 13(2), 530–544, available at: <https://doi.org/10.1093/icon/mov028>
- Bogdanovskii, A. (2006) *Mozhet li oshibat'sya Konstitutsionnyi sud?* [Can the Constitutional Court be wrong?]. *Zakonnost'*. No. 8. 32–36. (in Russian).
Богдановский А. Может ли ошибаться Конституционный суд? // Законность. 2006. № 8. С. 32–36.
- Bondar', N.S. (2005) *Vlast' i svoboda na vesakh konstitutsionnogo pravosudiya: zashchita prav cheloveka Konstitutsionnym Sudom Rossiiskoi Federatsii* [Power and freedom on the scales of constitutional justice: protection of human rights by the Constitutional Court of the Russian Federation]. Moscow, Justicinform Publ. (in Russian).

- Бондарь Н.С.* Власть и свобода на весах конституционного правосудия: защита прав человека Конституционным Судом Российской Федерации. М.: Юстицинформ. 2005. 592 с.
- Brunner, L. (2018) Digital communications and the evolving right to privacy. In M. Land, J. Aronson (eds.), *New Technologies for Human Rights Law and Practice* (217–242). Cambridge, Cambridge University Press. doi:10.1017/9781316838952.010
- Chechetin, A. (2005) Ogranichenie tainy svyazi [Limiting the secrecy of communication]. *Zakonnost'*. (7), 38–40. (in Russian).
- Чечетин А.* Ограничение тайны связи // Законность. 2005. № 7. С. 38–40.
- Dedov, D., Jakushev, M., Belov, S., Golovko, L., Bogush, G., Balytnikov, V., Soboleva, A., Sekretareva, N., Koroteev, K. (2018) Blokirovka Telegram v Rossii: kak obespechit' tainu perepiski? [Blocking Telegram in Russia: how to ensure privacy of correspondence?]. *Zakon*. (4), 18–28. (in Russian).
- Дедов Д., Якушев М., Белов С., Головкин Л., Богущ Г., Балытников В., Соболева А., Секретарева Н., Коротеев К.* Блокировка Telegram в России: как обеспечить тайну переписки? // Закон. 2018. № 4. С. 18–28.
- Drewry, L. (2016) Crime without culprits: why the European Union needs data protection, and how it can be balanced with the right to privacy. *Wisconsin International Law Journal*. Spring. 37 (1), available at: <https://wilj.law.wisc.edu/issues/> (Accessed 02 March 2020).
- Gushev, M.E., Shuvalova, A.M. (2015) The restriction of constitutional rights of missing citizens. *Historical and Social-educational idea*. 7(4), 64–66. DOI: 10.17748/2075-9908.2015.7.4.064-066. (in Russian).
- Гущев М.Е., Шувалова А.М.* Ограничение конституционных прав граждан, пропавших без вести // Историческая и социально-образовательная мысль. 2015. Том 7. № 4. С. 64–66. DOI: 10.17748/2075-9908.2015.7.4.064-066.
- Hoboken, J., Zuiderveen Borgesius, F. (2015) Scoping electronic communication privacy rules: data, services and values. *Journal of Intellectual Property, Information Technology and E-Commerce Law*. 6 (198), para 1, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2777156 (Accessed 07 June 2020).
- Kufleva, V.N., Kubrak, V.S. (2018) Problems of realization of the right for the mystery of correspondence in messengers: theoretical and komparativistsky aspects. *Humanities, social-economic and social sciences*. (10), 153–157. (in Russian).
- Куфлева В.Н., Кубрак В.С.* Проблемы реализации права на тайну переписки, в мессенджерах: теоретический и компаративистский аспекты // Гуманитарные, социально-экономические и общественные науки. 2018. № 10. С. 153–157.
- Nevzgodina, E.L. (2012) Yuridicheskaya sushchnost' predstavitel'stva kak universal'noi i unikal'noi formy posrednichestva [The legal essence of representation as a universal and unique form of mediation]. *Herald of Omsk University. Series «Law»*. 2 (31), 121–129. (in Russian).
- Невзгодина Е.Л.* Юридическая сущность представительства как универсальной и уникальной формы посредничества // Вестник Омского университета. Серия «Право». 2012. № 2 (31). С. 121–129.
- Papakonstantinou, V., Hert, P. (2011) The amended EU Law on ePrivacy and electronic communications after its 2011 implementation; new rules on Data protection, Spam, Data breaches and protection of intellectual property. *The John Marshall Journal of Computer & Information Law*, available at: <https://repository.jmls.edu/jitpl/vol29/iss1/2/> (Accessed 10 June 2020).
- Post, R.C. (2017) Data privacy and dignitary privacy: Google Spain, the right to be forgotten, and the construction of the public sphere. (April 15, 2017). *Duke Law Journal*. Forthcoming, Yale Law School, Public Law Research Paper. (598), available at: <http://dx.doi.org/10.2139/ssrn.2953468>. (Accessed 02 June 2020).

- Rego, A.V., Matskevich, A.Yu. (2019) The problem of access of antitrust authorities to secrecy of communication. *Russian competition law and economy*. (3), 16–19. (in Russian).
Рего А.В., Мацкевич А.Ю. Проблема доступа антимонопольных органов к тайне связи // Российское конкурентное право и экономика. 2019. № 3. С. 16–19.
- Soldatova, V.I. (2020) Protection of personal data in digital environment. *Lex Russica*. (2), 33–43. (in Russian).
Солдатова В.И. Защита персональных данных в условиях применения цифровых технологий // Lex russica. 2020. № 2. С. 33–43.
- Tenishev, A.P. (2018) On antitrust cybercrimes, access to secret information and the digital special unit. *Competition and Law Journal*. (5), 14–20. (in Russian).
- Тенишев А.П.* Об антимонопольных киберпреступлениях, доступе к тайнам и цифровом спецподразделении // Конкуренция и право. 2018. № 5. С. 14–20.
- Tereshhenko, L.K. (2016) Otdel'nye voprosy, vznikayushchie v sudebnoi praktike pri primenenii norm o taine svyazi [Certain issues arising in judicial practice when applying the rules on the secrecy of communication]. *Kommentarii sudebnoi praktiki* [Certain issues that arise in judicial practice when applying the rules on communication privacy. Commentary on judicial practice] Is. 21. In: Jaroshenko, K.B, Moscow, Institute of Legislation and Comparative Law under the Government of the Russian Federation: INFRA-M Publ. 145–153. (in Russian).
Терещенко Л.К. Отдельные вопросы, возникающие в судебной практике при применении норм о тайне связи // Комментарий судебной практики. Вып. 21 / К.Б. Ярошенко, М.К. Белобабченко, А.Ф. Ефимов [и др.]; отв. ред. К.Б. Ярошенко. М.: Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации: ИНФРА-М, 2016. С. 145–153.
- Zuiderveen Borgesius, F., Steenbruggen, W. (2018) The right to communications confidentiality in Europe: protecting trust, privacy, and freedom of expression. *Theoretical Inquiries in Law, Forthcoming*, available at: <https://ssrn.com/abstract=3152014> (Accessed 17 May 2020).
- Vaipan, V.A., Egorova, M.A. (eds.) (2019) *Pravovoe regulirovanie jekonomicheskikh otnoshenij v sovremennykh uslovijah razvitija cifrovoj jekonomiki* [Legal regulation of economic relations in modern conditions of digital economy development]. In: Vaipan V.A., Egorova M.A. Moscow, Justicinform Publ. (in Russian).
Правовое регулирование экономических отношений в современных условиях развития цифровой экономики / Отв. ред. Вайпан В.А., Егорова М.А. М.: Юстицинформ. 2019. 376 с.

Об авторе:

Изотова Анжелика Николаевна — ведущий юрисконсульт, Публичное акционерное общество «Мобильные ТелеСистемы», аспирант, кафедра информационного права, Национальный исследовательский университет «Высшая школа экономики»; 101000, Российская Федерация, г. Москва, ул. Мясницкая, д. 20

ORCID ID: 0000-0002-2880-3900, SPIN-код 4884-3860

e-mail: anzheliki@rambler.ru

About the author:

Anzhelika N. Izotova — senior legal adviser of Mobile TeleSystems Public Joint Stock Company, postgraduate student, the Department of Information Law, National Research University Higher School of Economics; 20 Myasnitskaya Ulitsa, Moscow, 101000, Russian Federation

ORCID ID: 0000-0002-2880-3900, SPIN-code 4884-3860

e-mail: anzheliki@rambler.ru