НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

НАУЧНЫЙ ДОКЛАД

по результатам подготовленной научно-квалификационной работы (диссертации)

тема диссертации:

Правовое регулирование тайны связи в современных условиях

ФИО: **Изотова Анжелика Николаевна**

Направление подготовки: **40.06.01 Юриспруденция**

Профиль (направленность) программы: **12.00.13 – Информационное право**

Аспирантская школа по праву

Аспирант _____/ А.Н. Изотова

Научный руководитель _____/ к.ю.н., доцент Н.А. Дмитрик

Москва, 2021

Аннотация

Исследование посвящено правовому регулированию тайны связи как института информационного права. Институт тайны связи с появлением новых коммуникационных технологий, цифровизацией общества, трансформируется и расширяется, что требует уточнения теоретических представлений о нем, а также актуализации и гармонизации законодательной базы.

В работе проведен анализ доктринальных представлений, законодательства и имеющейся судебной практики о тайне связи, ее содержании, особенностях правового статуса субъектов тайны связи, условиях доступа к сведениям, составляющим тайну связи, и их обработки.

В результате исследования определен контекстный характер тайны связи, влияющий на ее содержание. Отмечено изменение роли информационных посредников, обеспечивающих работу коммуникационных сервисов (операторы связи, организаторы распространения информации в сети «Интернет»)[1] от пассивно-нейтральной к активной роли по отношению к коммуникационному трафику, что может сопровождаться ограничением тайны связи пользователей. Определены возможные условия обработки сведений, составляющие тайну связи, информационными посредниками с точки зрения риск-ориентированного подхода и контекстной целостности конфиденциальной информации. Полагаем, что это в свою очередь позволит решить часть проблем, связанных с нахождением баланса между интересами человека, государства и информационных посредников.

[1] В исследовании идет речь только об информационных посредниках, обеспечивающих коммуникации (оказывающих услуги связи, организующих работу коммуникационных сервисов) и обязанных обеспечить защиту тайны связи.

Объектом исследования являются общественные отношения в сфере коммуникаций, связанные с тайной переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (тайны связи).

Предметом исследования являются правовые аспекты регулирования тайны связи как правового режима информации ограниченного доступа, условий ее обеспечения и защиты.

Степень научной разработанности темы и теоретическая основа исследования. Стабильный интерес к исследованию правовых вопросов обеспечения конфиденциальности коммуникаций сохраняется на протяжении последнего столетия. Однако в последнее десятилетие научный интерес к этой теме существенно возрос в связи со стремительным распространением различных форм коммуникаций.

Теоретической основой настоящего исследования стали работы российских и зарубежных ученых в области информационного права и иных отраслевых правовых наук.

Общетеоретические положения о правовом статусе человека, балансе частных и публичных интересов, неприкосновенности частной жизни, неотъемлемой частью чего является тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений как одной из составляющих правового статуса личности, изложены в трудах отечественных ученых в области теории права, конституционного права, таких как С.С. Алексеев, М.В. Баглай, С.Н. Братусь, Т.А. Васильева, Н.В. Витрук, Г.А. Гаджиев, О.Е. Кутафин, В.В. Лазарев, Е.А. Лукашева, Ю.И. Малевич, А.В. Малько, Н.И. Матузов, И.Л. Петрухина, А.Я. Сухарев, О.И. Тиунов, В.Е. Чиркин, Б.С. Эбзеев и других, а также зарубежных авторов, например, Дж. Беллами, А. Бэкси, К. Васак, Д. Гомьен, Л. Зваак, Д. Харрис, К. Экштайн.

Труды Л.К. Терещенко, А.В. Минбалеева, Г.Г. Камаловой, В.А. Северина, Н.И. Петрыкиной сформировали научные представления о

правовой природе информации и её правовом режиме. В.В. Архипов, Н.А. Дмитрик, В.Б. Наумов, А.И. Савельев, Э.В. Талапина, А.В. Туликов, а также Э. Граттон, Х. Ниссенбаум, Р. Познер, Д. Солове и другие внесли вклад в исследование эволюции прав человека (в том числе приватности) и институтов информационного права.

Непосредственно вопросы правового регулирования тайны связи прослеживаются в работах В.А. Вайпана, В.Ю. Волкова, Ю.В. Гаврилина, Л.И. Ивченко, Е.С. Лапина, К.И. Попова, Н.Ю. Рязанова, В.Ю. Стельмаха, Л.К. Терещенко, А.В. Черенкова, А.Е. Чечетина, Н.Г. Шурухнова, А.В. Юшкевича и др.

В последние десятилетия по проблематике, затрагивающей тайну связи, был защищен ряд диссертаций, но анализ этих работ позволяет сделать вывод о том, что исследования в основном касались тайны связи как личной тайны человека с точки зрения конституционного права, а также уголовного, уголовно-процессуальных аспектов тайны связи. Исследования проблем тайны связи с точки зрения институтов информационного права, перспектив развития с учетом изменений законодательства и тенденции глобальной информатизации общества, в последние годы не проводилось.

Актуальность темы исследования.

В информационном обществе претерпевают изменения многие сферы общественной жизни, в том числе и сфера коммуникаций. Скачок в развитии информационной инфраструктуры, совершенствование современных информационных технологий, появление новых форм коммуникаций, основанных на обмене данными в сети «Интернет», международный характер коммуникаций, реализация программы Цифровой экономики оказывают влияние на институт тайны связи и приводят к необходимости по-другому взглянуть на его правовую природу, содержание.

С одной стороны, в условиях цифровизации коммуникаций возрастает значение информационной безопасности пользователей услугами связи, коммуникационными сервисами, повышаются риски нарушения тайны связи,. Нельзя не отметить, что обеспечение информационной безопасности является стратегической задачей развития цифровой экономики во многих государствах, включая Российскую Федерацию[2]. Информационная безопасность и правовое регулирование цифровой среды отнесены к базовым направлениям построения цифровой экономики и находятся друг с другом в тесной взаимосвязи. С другой стороны, реализация программы Цифровой экономики ставит вопрос о пересмотре правовых механизмов доступа разного рода данным, в том числе к сведениям, составляющим тайну связи, условий их обработки. Помимо этого, изменяется подход государства к роли информационных посредников, участвующих в организации коммуникаций, возложению на них дополнительных функций. Все это подчеркивает назревшую необходимость создания действенного механизма регулирования тайны связи, учитывающего интересы всех субъектов.

Научная новизна работы заключается в том, что она представляет собой исследование правовых аспектов тайны связи как информационно-правовой категории. Выявленные особенности содержания тайны связи, тенденции развития тайны связи в информационном обществе, выработанные условия обработки сведений, составляющих тайну связи, могут послужить теоретической базой для дальнейших исследований в области правового регулирования тайны связи и информационного права в целом, как в России, так и за рубежом.

---

[2] Паспорт национального проекта «Национальная программа "Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7). URL: https://digital.gov.ru (дата обращения: 20.09.2021).

Цель исследования состоит в уточнении теоретических положений о тайне связи, выявлении тенденций развития тайны связи в связи с глобальной информатизацией общества.

Достижение поставленной цели возможно посредством решения комплекса следующих **задач:**

- определить правовую природу и содержание тайны связи применительно к современным условиям,

- выработать критерии отнесения информации к сведениям, составляющим тайну связи;

- определить роль информационных посредников в обеспечении тайны связи как профессиональной тайны;

- исследовать международные подходы и зарубежный опыт в вопросах правового регулирования тайны связи;

- выработать подходы к модернизации тайны связи, определить условия расширения доступа, обработки сведений, составляющих тайны связи.

Методологическую основу исследования составили как общенаучные методы познания (диалектический, анализ и синтез, индукция и дедукция, аналогия), так и специальные научные методы (формально-юридический, сравнительно-правовой). В сочетании указанные методы позволили полно и объективно изучить вопросы правового регулирования тайны связи и решить поставленные в исследовании задачи.

Эмпирическая база исследования включает действующие нормативно-правовые акты Российской Федерации и зарубежных стран, документы международных организаций, акты судов, проекты нормативно-правовых актов, а также доктринальные источники.

Основные результаты исследования и положения, выносимые на защиту.

1. Тайна связи носит интерконтекстный характер.

Контекстная целостность тайны связи основана на концепции Х. Ниссенбаум[3], базирующейся на западных доктринах разумного ожидания[4] и третьей стороны[5]. Концепция контекстной целостности применительно к обработке информации заключается в том, что все события (сбор, использование, распространение информации) происходят в конкретном контексте, который и определяет применимый набор норм, роли, ожидания и вытекающие из этого действия. Это в полной мере применимо и к тайне связи. Пользуясь услугами связи или коммуникационным сервисом, субъект осознает, что вверяет свои сообщения информационному посреднику. При этом контекст коммуникации предполагает, что информация о такой коммуникации и ее содержании останется в тайне от третьих лиц. Контекст коммуникаций, обеспеченных информационным посредником, также определяет условия обработки информации о коммуникации в целях обеспечения самой коммуникации.

В этой связи представляются показательными результаты социологического исследования в отношении совместимости услуг межличностной связи[6]. Исследование показало, что пользователи разных

---

[3] Nissenbaum H. Privacy as Contextual Integrity. Washington Law Review. 2004. Vol. 79. Iss. 1. P. 119–158. URL: https://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf (дата обращения 23.09.2021).

[4] Доктрина разумного ожидания сформирована в деле Katz v. United States (389 US 347 (1967). URL: https://supreme.justia.com/cases/federal/us/389/347/ (дата обращения 23.09.2021). Действие доктрины проявляется посредством проведения теста, состоящего из 2 этапов: оценки фактического ожидания человеком секретности и оценки объективной (разумной) секретности в конкретной ситуации. Впервые тест был сформулирован в деле Smith v. Maryland (442 US 735 (1979)). URL: https://supreme.justia.com/cases/federal/us/442/735/ (дата обращения 23.09.2021).

[5] Доктрина третьей стороны заключается в том, что лицо не вправе рассчитывать на конфиденциальность его коммуникаций, когда добровольно предоставляют свои данные третьей стороне (оператору связи, интернет-провайдеру). Доктрина была установлена в деле Smith v. Maryland (442 U.S. 735 (1979)). URL: https://tile.loc.gov/storage-services/service/ll/usrep/usrep442/usrep442735/usrep442735.pdf (дата обращения 24.09.2021).

[6] Arnold R., Schneider A., Lennartz J. Interoperability of interpersonal communications services – A consumer perspective. Telecommunication Policy. 2020. 44. URL: https://doi.org/10.1016/j.telpol.2020.101927 (дата обращения 28.09.2021).

сервисов обмена мгновенными сообщениями, не совместимых друг с другом[7], осознанно используют это свойство сервисов для разных коммуникаций. Иными словами, пользователи, выбирая тот или иной коммуникационный сервис, формируют контекст коммуникаций в широком смысле, учитывая доверие к этому конкретному сервису, цель коммуникации, свою социальную роль в этой коммуникации. В одном контексте может быть выбран один сервис, в другом контексте – совсем другой сервис.

Контекстный характер тайны связи также прослеживается и при определении состава сведений, составляющих тайну связи, и подлежащих защите посредством установления в отношении них специального правового режима информации. Так, тайной связи охватываются все сведения, которые определяются по контексту коммуникаций: как сами сообщения, так и непосредственно связанные с ними сведения, полученные, сформированные у оператора связи, организатора коммуникационного сервиса в связи с оказанием услуг связи, обеспечением коммуникаций. Этот подход нашел отражение в Определении Конституционного суда РФ от 02.10.2003 г. № 345-О, ставшим прецедентным в отношении тайны связи в России, а также в законодательстве и судебной практике зарубежных стран.

2. <u>В современных условиях востребована активная роль информационных посредников, участвующих в обеспечении коммуникаций, в отношении обработки передаваемых сообщений (контента), сопряженная с усилением ответственности информационных посредников.</u>

Одна из особенностей тайны связи кроется в сфере ее применения – коммуникациях, в обеспечении которых участвует третье лицо – информационный посредник (оператор связи, организатор распространения информации в сети «Интернет» и т.п.).

---

[7] Сервисы обмена мгновенными сообщениями основаны на несовместимых между собой протоколах, что не позволяет им взаимодействовать друг с другом. Обмен сообщениями осуществляется исключительно внутри сервиса.

Информационные посредники в области коммуникаций оказывают услуги по сбору, обработке, передаче и доставке информации, предоставленной иными лицами, без ее изменения в процессе передачи[8], то есть традиционно играют пассивную или нейтральную роль по отношению к передаваемому посредством них трафику[9]. Такому положению информационных посредников свойственен режим ограниченной ответственности, для которого характерно:

1) отсутствие ответственности посредников за контент третьих лиц при условии, что они не изменяют этот контент и не осведомлены о его незаконном характере;

2) отсутствие общих обязательств по мониторингу контента.

Предполагалось, что ограничение ответственности информационных посредников в отношении контента, размещенного посредством них, стимулирует инновации, обеспечит повышение эффективности Интернета, разнообразия и качества интернет-услуг[10]. Сейчас эти сервисы коммуникаций уже не нуждаются в подобном стимулировании. Поэтому отмечается активное внедрение механизмов вторичной ответственности информационных посредников.

Также на информационного посредника возлагается обязанность по мониторингу контента для выявления правонарушений, и при невыполнении или некачественном выполнении обязанности мониторинга с стороны информационного посредника, он считается способствующим совершению правонарушения. Соответственно принципы «безопасной гавани» в такой

---

[8] Ст. 17 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»// СПС «КонсультантПлюс».

[9] Войниканис Е.А. Право интеллектуальной собственности в цифровую эпоху: парадигмы баланса и гибкости. – М.: Юриспруденция, 2013. 552 с.

[10] Kuczerawy A. From 'Notice and Takedown' to 'Notice and Stay Down': Risks and Safeguards for Freedom of Expression. Oxford Handbook of Online Intermediary Liability. Edited by G. Frosio. 2020. DOI: 10.1093/oxfordhb/9780198837138.013.27 (дата обращения: 12.09.2021)

ситуации не могут быть применены. Такой переход неуклонно набирает силу и превращается в основной подход к ответственности посредников[11].

Большинство существующих механизмов борьбы с нарушениями в информационной сфере касаются нарушения авторских прав. Со временем некоторые страны расширили сферу действия подобных механизмов на другие виды нарушений. Обычно механизмы вторичной ответственности не были сопряжены с ограничением права на тайну связи. Но совсем недавно принят Регламент ЕС 2021/1232 о временном отклонении от отдельных положений Директивы ЕС 2002/58/ЕС для борьбы с сексуальной эксплуатацией детей[12]. Регламент прямо предусматривает ограничение права на тайну связи, предусмотренного Директивой (ЕС) 2018/1972[13]. В соответствии с Регламентом, в течение 3 лет с даты его принятия поставщики услуг межличностных коммуникаций, не зависящих от номера телефона, (то есть организаторы мессенджеров, социальных сетей, электронной почты и т.п., но не операторы связи) в установленном порядке получают право осуществлять мониторинг сообщений пользователей в целях обнаружения и удаления материалов, представляющих сексуальную эксплуатацию детей, блокировать учетные записи нарушителей, приостанавливать, прекращать оказание услуг отдельным пользователям, а также сообщать о таких правонарушениях в уполномоченный орган. Фильтрация трафика может осуществляться для построения моделей выявления правонарушений без постоянного мониторинга переписки. Для минимизации рисков нарушения тайны связи, предотвращения злоупотреблений со стороны информационного посредника

---

[11] Frosio G., Mendis S. Monitoring and Filtering: European Reform or Global Trend? Oxford Handbook of Online Intermediary Liability. Edited by Giancarlo Frosio. 2020. DOI:10.1093/oxfordhb/9780198837138.013.28 (дата обращения: 12.09.2021)

[12] Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R1232 (дата обращения: 12.09.2021)

[13] Directive (EU) 2018/1972 of the European Parliament and the Council of 11 Dec 2018 establishing European Electronic Communications Code. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972&from=EN (дата обращения: 12.09.2021)

Регламентом предусмотрен ряд условий осуществления мониторинга переписки, а также требования к технологии мониторинга.

Помимо перечисленных обязательств по мониторингу контента, переписки, сопряженных с вторичной ответственностью информационных посредников, в области тайны связи имеет место наделение информационных посредников обязанностями по хранению сообщений и информации о них. В большинстве развитых стран действуют подобные нормы в целях содействия правоохранительным органам в обнаружении и расследовании преступлений[14]. Так, в России «законом Яровой»[15] на операторов связи и организаторов распространения информации в сети «Интернет» возложены обязанности по фиксации и хранению информации о пользователях, о совершенных ими соединениях, а также содержания таких соединений.

3. Обработка данных, составляющих тайну связи, информационными посредниками допустима при соблюдении условий, исключающих причинение вреда.

В связи с возложением государством на информационных посредников дополнительных обязанностей встает вопрос о свободе ведения бизнеса и компенсации издержек информационных посредников. Право на свободное ведение бизнеса закреплено в ст. 16 Хартии ЕС об основных правах[16]. Это относительно молодое право, причем отмечается, что оно не имеет широкого признания, что позволяет государствам свободно ограничивать его[17], что мы и наблюдаем в ситуации с информационными посредниками. При этом

---

[14] Riordan J. A Theoretical Taxonomy of Intermediary Liability. Oxford Handbook of Online Intermediary Liability. Edited by G. Frosio. 2020. DOI: 10.1093/oxfordhb/9780198837138.013.3 (дата обращения: 21.09.2021).

[15] 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» // СПС «КонсультантПлюс».

[16] Charter of Fundamental Rights of the European Union (2016/C 202/02). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12016P/TXT&from=EN#d1e32-391-1 (дата обращения: 20.09.2021)

[17] Geiger C., Frosio G, Izyumenko E. Intermediary Liability and Fundamental Rights. Oxford Handbook of Online Intermediary Liability. Edited by G. Frosio. 2020. DOI: 10.1093/oxfordhb/9780198837138.013.7 (дата обращения: 21.09.2021).

экономическое влияние на деятельность информационных посредников колоссально.

Определенную пользу может принести механизм добровольного принятия информационным посредником обязанностей по выявлению и пресечению нарушений в информационной среде посредством мониторинга переписки или звонков. Так, технологии, сходные с предусмотренными Регламентом ЕС 2021/1232 для целей защиты детей от сексуального насилия, могут применяться и для выявления других нарушений. Этот подход позволил бы информационным посредникам коммерциализировать деятельность по мониторингу данных, относящихся к тайне связи, минимизировав возможный ущерб от обязательного мониторинга, предусмотренного законодательством.

Однако для признания допустимой обработки информационными посредниками сведений, составляющих тайну связи, необходимо обеспечить защиту тайны связи. Эффективным может быть риск-ориентированный подход, описанный Э. Граттон[18], для исключения либо минимизации вероятности наступления вреда от обработки сведений, составляющих тайны связи.

Согласно этому подходу, обработка конфиденциальной информации может причинить лицу, чья информация обрабатывается, субъективный вред (психологический, эмоциональный ущерб в виде страдания, унижения, стыда, смущения, гнева, ощущения постоянного наблюдения и пр.) и объективный вред (физический, финансовый вред, неравенство в результате дискриминации, профилирования, поведенческого маркетинга и т.д.). Д. Солове в таксономии приватности выделил различные типы действий, которые могут причинить вред приватности: сбор информации, обработка информации, распространение информации и личные вторжения[19]. Опираясь на это, Э. Граттон использовала первые три типа действий, которые относятся

[18] Gratton E. Understunding personal information: managing privacy risks. Markham: LexisNexis, 2013. 515 p.
[19] Solove D. A Taxonomy of Privacy. University of Pennsylvania Law Review. 2006, Vol. 154, No. 3, pp. 477-564. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=667622 (дата обращения: 20.09.2021)

именно к обработке конфиденциальной информации. В исследовании продемонстрировано, что вид возможного вреда напрямую связан с типом обработки информации: сбор информации приводит к субъективному ущербу, использование - к объективному, раскрытие – к субъективному вреду, а также к объективному вреду в результате использования информации третьими лицами, получившими доступ к ней в результате раскрытия. Отмечено, что для субъективного вреда характерны критерии: возможность идентификации лица, которому принадлежит информация; чувствительность информации для лица; степень доступности информации для третьих лиц. Для объективного вреда существует один критерий – причинит ли использование информации вред или нет.

Применяя риск-ориентированный подход к обработке информационным посредником сведений, составляющих тайну связи, условия допустимости обработки (мониторинга) контента, переписки, звонков могут быть следующими.

Сбор данных уже сейчас осуществляется информационным посредником в силу обеспечения работы коммуникационных сервисов, поэтому субъективный вред не причиняется.

Использование данных сопряжено с субъективным и объективным ущербом, поэтому необходима разработка комплекса мер по предотвращению такого ущерба. В части предотвращения субъективного ущерба потребуется исключение возможности идентификации, использование наименее чувствительных данных (например, данных о соединениях, без вмешательства в их содержание), обработка данных без участия человека, но с возможностью контроля с его участием. В части исключения вероятности причинения объективного вреда потребуется получение согласия лица, чьи данные планируются к обработке. Помимо указанных мер, следует обеспечить соблюдение общих условий обработки конфиденциальной информации,

которые подробно описаны в законодательстве о защите персональных данных.

Распространение сведений, составляющих тайну связи, не допустимо в силу прямого запрета в международных документах, конституционных нормах, закрепляющих тайну связи, а также в связи с тем, что распространение сведений с высокой вероятностью может повлечь как субъективный, так и объективный ущерб.

4. При обработке информационными посредниками сведений, составляющих тайну связи, а особенно при таком способе обработки, как использование, должна учитываться концепцию контекстной целостности.

При оценке допустимости обработки информационными посредниками сведений, составляющих тайну связи, должен быть учтен контекст ее обработки, о котором шла речь ранее. Это не значит, что обработка возможна только для обеспечения коммуникаций и цель обработки не может быть изменена. Н.А. Дмитрик, рассматривая вопрос о перемещении информации между контекстами (когда информация, предоставленная для одной цели, может обрабатываться для другой цели), обратил внимание на согласие субъекта, чья информация обрабатывается, как на инструмент, который обеспечивает связь между субъектом и контекстом[20]. То есть при согласии субъекта с изменением контекста может иметь место обработка информации. В литературе отмечается, что согласие в таких случаях является единственной защитой от нарушения обязанностей в отношении вторжения или публичного раскрытия информации[21].

При выражении согласия с обработкой своих данных, данных о своей переписке, лицо имеет возможность найти баланс между своим правом на

[20] Дмитрик Н.А. История, смысл и перспективы институту персональных данных//Вестник гражданского права. 2020. № 3. Том 20. С. 56. URL: https://doi.org/10.24031/1992-2043-2020-20-3-43-82 (дата обращения: 14.09.2021)

[21] Hubbard P. The Need for Privacy Torts in an Era of Ubiquitous Disclosure and Surveillance. In: Cudd A., Navin M. (eds) Core Concepts and Contemporary Issues in Privacy. AMINTAPHIL: The Philosophical Foundations of Law and Justice, vol 8. Springer, Cham. 2018. P. 148. URL: https://link.springer.com/chapter/10.1007%2F978-3-319-74639-5_10 (дата обращения: 12.09.2021)

тайну переписки и иными правами. Так, пользователь услугами связи, мессенджера может не давать согласия на обработку его переписки и не иметь психологического дискомфорта от ее мониторинга, а может дать такое согласие и не получать, например, спам, выявленный посредством мониторинга переписки, или получить сервис по фильтрации звонков, поступающих от мошенников, или дать согласие и получить скидку на услуги, а информационный посредник, используя данные о геолокации, разрабатывать новые сервисы.

Наряду с возможностью выразить согласие на обработку данных, лицо вправе запретить обработку его данных. Так, в некоторых сервисах обмена сообщениями существует возможность сквозного шифрования сообщений[22]. По своей сути этот инструмент является явным запретом пользователя на использование его сообщений. Это вступает в противоречие с доктриной третьей стороны, которая предполагает, что лицо не вправе рассчитывать на конфиденциальность его коммуникаций, когда добровольно предоставляет свои данные информационному посреднику. Однако случаи, когда пользователь коммуникационного сервиса явно выражает намерение скрыть от информационного посредника свои сообщения, подпадают под действие «контейнерной доктрины»[23]. Судами такая доктрина признается обладающей большей конституционной защитой. В упомянутом ранее Регламенте ЕС 2021/1232 прямо указано, что шифрование сообщений является важным инструментом, гарантирующим их безопасность и конфиденциальность и не может быть запрещено. Контейнерная доктрина влечет за собой применение доктрины разумного ожидания, когда пользователь, защитивший свои сообщения, ожидает, что его сообщения не будут доступны информационному посреднику.

---

[22] Условия конфиденциальности и безопасности WhatsApp. Сквозное шифрование. URL: https://faq.whatsapp.com/general/security-and-privacy/end-to-end-encryption/?lang=ru (дата обращения: 15.09.2021)

[23] Fairfield J.A.T. Owned: Property, Privacy, and the New Digital Sendrom. 2017. P. 127. URL: https://doi.org/10.1017/9781316671467 (дата обращения: 12.09.2021)

5. Выработка на международном уровне минимальных требований к защите сведений, составляющих тайну связи, является необходимым условием обеспечения тайны связи в условиях глобализации коммуникационных сервисов.

Современные коммуникационные сервисы, широко используемые по всему миру, в том числе в России, организованы компаниями, зарегистрированными в соответствии с законодательством разных стран (Facebook, Whats App – в США, Viber - в Люксембурге и т.д.). Это, безусловно, актуализирует проблему применимого права для обеспечения тайны связи в таких сервисах, обостряемую различающимися правовыми подходами к обработке сведений, составляющих тайну связи, в странах, чьи граждане используют коммуникационные сервисы.

Так, американский закон о конфиденциальности электронных сообщений (Electronic Communications Privacy Act of 1986)[24] устанавливает более широкий перечень случаев обработки сведений, составляющих тайну связи, чем законодательство России и Европейского союза, активно используя получение согласия абонента в ряде случаев. Закон об электронных коммуникациях Эстонии (Electronic communication Act)[25], как и американский аналогичный закон, предоставляет операторам связи широкие возможности обработки сведений, составляющих тайну связи, но наряду с получением согласия на обработку данных, использует уведомление абонента о целях обработки с предоставлением ему возможности отказа от такой обработки. Закон Германии «О телекоммуникациях» (Telekommunikationsgesetz)[26] 2004 г. возлагает обязанность по обеспечению тайны связи не только на операторов связи, но и на иных лиц, участвующих в оказании услуг связи, расширяя перечень лиц, имеющих доступ к сведениям о коммуникациях.

---

[24] Electronic Communications Privacy Act. URL: https://www.law.cornell.edu/uscode/text/18/part-I/chapter-119 (дата обращения 23.09.2021).
[25] Electronic communication Act. URL: https://www.riigiteataja.ee/en/eli/501042015003/consolide (дата обращения 10.09.2021).
[26] Telekommunikationsgesetz. URL: https://www.gesetze-im-internet.de/tkg_2004 (дата обращения 23.09.2021).

В связи с этим глобализация коммуникационных процессов требует выработки мер, обеспечивающий минимальный уровень защиты данных, подпадающих под режим тайны связи.

В качестве отправной точки для этого может быть предложена концепция «безопасной гавани» конфиденциальности (The Safe Harbour Privacy Principles[27]), положенная в основу европейского регулирования трансграничной передачи персональных данных[28]. В частности, к принципам концепции относятся: уведомление субъекта данных об условиях обработки; возможность выбора при даче согласия на обработку данных; передача третьим лицам в случаях, когда это необходимо; доступ субъекта к своим данных; целостность данных (контекстная целостность), наличие доступных для субъекта средств защиты. Не все перечисленные принципы применимы для обеспечения тайны связи (как, например, передача третьим лицам, которая в России допускается лишь на основании решения суда и в случаях, предусмотренных законом), другие - требуют проработки для эффективной защиты сведений, составляющих тайну связи.

Теоретическая значимость исследования состоит в расширении научных представлений о тайне связи как информационно-правовой категории. Результаты исследования могут быть использованы в теоретических разработках проблем тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений.

Практическая значимость исследования заключается в предложении направлений развития нормативно-правового регулирования в сфере обеспечения тайны связи, а также обусловлена ее направленностью на

---

[27] 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce. URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML (дата обращения 25.09.2021).

[28] 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). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02002L0058-20091219 (дата обращения 24.09.2021).

обеспечение единообразного и точного применения правовых норм участниками правоотношений (в том числе судами, государственными и муниципальными органами, операторами связи), исключение ошибок в правоприменении, связанных с неверным толкованием содержания тайны связи, условий ее ограничения, правил доступа к сведениям, составляющим тайну связи, их обработки. Результаты исследования также могут быть использованы в учебном процессе, в том числе в рамках специальных дисциплин.

Апробация результатов исследования

Диссертация выполнена в Департаменте теории права и межотраслевых наук Факультета права Национального исследовательского университета «Высшая школа экономики». Положения диссертационного исследования нашли отражение в научных статьях[29], опубликованных в научных изданиях, в том числе рекомендованных ВАК Министерства образования и науки Российской Федерации, входящих в список НИУ ВШЭ журналов высокого уровня.

Основные положения и выводы научного исследования были представлены в докладах автора на научных конференциях по проблемам информационного права[30].

Отдельные положения исследования использовались в преподавательской деятельности автора на образовательных программах

---

[29] 1) Изотова А.Н. Отдельные вопросы обеспечения тайны связи // Евразийский юридический журнал, 2018, № 1, с. 300-302; 2) Изотова А.Н. Право на тайну связи абонента и пользователя // Юридическая наука. 2020. № 9. С. 55-58; 3) 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; 4) Izotova, A. (2021). The Right to Access to Privacy of Correspondence and Russian Judicial Practice. Legal Issues in the Digital Age, 1(1), 160-168; 5) Изотова А.Н. Ограничение права на тайну связи в условиях пандемии COVID-19 // Вестник Воронежского государственного университета. Серия: Право (*в печати*); 6) Изотова А.Н. Субъекты правового режима тайны связи в условиях цифровой экономики // Актуальные проблемы российского права (*в печати*); 7) Изотова А.Н. Тайна связи: обработка данных информационным посредником //Законодательство. 2022. № 1 (*в печати*).

[30] 1) IX Международная конференция "Право в цифровую эпоху", Москва, 21-22 октября 2019 г. Доклад на тему: "Современные тенденции развития регулирования тайны коммуникаций"; 2) XV Международная школа-практикум молодых ученых юристов "Конституция и модернизация законодательства", Москва, 27.05 - 05.06 2020 г. (10 модуль, 04.06.2020 г.). Доклад на тему "Ограничение тайны связи в условиях пандемии".

Факультета права НИУ ВШЭ[31], а также при участии в научно-исследовательских проектах НИУ ВШЭ[32].

Список использованных источников и литературы

1. Войниканис Е.А. Право интеллектуальной собственности в цифровую эпоху: парадигмы баланса и гибкости. – М.: Юриспруденция, 2013. 552 с.
2. Дмитрик Н.А. История, смысл и перспективы институту персональных данных//Вестник гражданского права. 2020. № 3. Том 20. С. 56. URL: https://doi.org/10.24031/1992-2043-2020-20-3-43-82 (дата обращения: 14.09.2021).
3. Собрание сочинений В.С. Соловьева/ Под. ред. С.М. Соловьева и Э.Л. Радлова. Том 8. - СПб: Книгоиздательское товарищество Просвещение, 1914. 722 с.
4. Arnold R., Schneider A., Lennartz J. Interoperability of interpersonal communications services – A consumer perspective. Telecommunication Policy. 2020. 44. URL: https://doi.org/10.1016/j.telpol.2020.101927 (дата обращения 28.09.2021).
5. Fairfield J.A.T. Owned: Property, Privacy, and the New Digital Sendrom. 2017. P. 127. URL: https://doi.org/10.1017/9781316671467 (дата обращения: 12.09.2021)
6. Frosio G., Mendis S. Monitoring and Filtering: European Reform or Global Trend? Oxford Handbook of Online Intermediary Liability. Edited by Giancarlo

[31] В рамках курса «Информационное право» (магистерская программа Факультета права ВШЭ «Право информационных технологий и интеллектуальной собственности» 2020-2021, магистерская программа Факультета права ВШЭ «Цифровое право» 2021-2022 гг.), научно-исследовательских семинаров (бакалаврская программа Факультета права ВШЭ «Юриспруденция» 2021 г.).

[32] 1) НИП (Международная лаборатория по праву информационных технологий и интеллектуальной собственности ВШЭ). Исследование зарубежного опыта правового регулирования управления данными, формирование предложений по совершенствованию правового регулирования управления данными для Российской Федерации в рамках реализации мероприятий по созданию национальной системы управления данными в рамках федерального проекта "Цифровое государственное управление" национальной программы "Цифровая экономика Российской Федерации" (2019 г.); 2) НИП (Институт права цифровой среды ВШЭ). Проблемы нормативно-правового регулирования тайны связи в условиях цифровой экономики: российский и международный опыт (2020 г.); 3) НИП (Институт права цифровой среды ВШЭ). Правовое регулирование цифровых платформ (2021 г.).

Frosio. 2020. DOI:10.1093/oxfordhb/9780198837138.013.28 (дата обращения: 12.09.2021).

7. Geiger C., Frosio G, Izyumenko E. Intermediary Liability and Fundamental Rights. Oxford Handbook of Online Intermediary Liability. Edited by G. Frosio. 2020. DOI: 10.1093/oxfordhb/9780198837138.013.7 (дата обращения: 12.09.2021).
8. Gratton E. Understunding personal information: managing privacy risks. Markham: LexisNexis, 2013. 515 p.
9. Kuczerawy A. From 'Notice and Takedown' to 'Notice and Stay Down': Risks and Safeguards for Freedom of Expression. Oxford Handbook of Online Intermediary Liability. Edited by G. Frosio. 2020. DOI: 10.1093/oxfordhb/9780198837138.013.27 (дата обращения: 12.09.2021).
10. Nissenbaum H. Privacy as Contextual Integrity. Washington Law Review. 2004. Vol. 79. Iss. 1. P. 119–158. URL: https://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf (дата обращения 23.09.2021).
11. Riordan J. A Theoretical Taxonomy of Intermediary Liability. Oxford Handbook of Online Intermediary Liability. Edited by G. Frosio. 2020. DOI: 10.1093/oxfordhb/9780198837138.013.3 (дата обращения: 12.09.2021).
12. Solove D. A Taxonomy of Privacy. University of Pennsylvania Law Review. 2006, Vol. 154, No. 3, pp. 477-564. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=667622 (дата обращения: 12.09.2021).