РОСКОМСВОБОДА

ОТЧЕТ

ЛУЧШИЕ МИРОВЫЕ ПРАКТИКИ ЗАЩИТЫ ЦИФРОВЫХ ПРАВ

НАД ОТЧЕТОМ РАБОТАЛИ:

САРКИС ДАРБИНЯН

МАРИЯ ПШЕНИЦЫНА

АННА КАРНАУХОВА

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

На рубеже XX-XXI веков развитие сети интернет приобрело колоссальное значение: его использование по всему миру и проникновение во все аспекты жизни человека достигло огромных масштабов. Электронные устройства стали постоянными спутниками людей, предоставляя им возможность круглосуточно пользоваться услугами и сервисами. Возникла новая область общественных отношений, основанная на цифровизации, и выделились связанные с ней «цифровые» права человека.

Цифровые права - это те же права человека, но в онлайне. В 2012 году (и снова в 2014 и 2016 годах) Совет ООН по правам человека согласился в резолюции, что «те же права, которые люди имеют в оффлайне, также должны быть защищены в интернете». Это означает, что вместо того, чтобы Организация Объединенных Наций пыталась определить новые права в онлайн пространстве, она рекомендовала распространить существующие права человека на киберпространство.

В российском праве термин "цифровые права" впервые появился в 2019 году, однако законодатель вложил в него совершенно иной смысл, значительно отличающийся от международной практики. Закон[1], вносящий в Гражданский кодекс РФ изменения, касающиеся регулирования цифровых прав, понимает в качестве таких прав обязательственные и иные права, содержание и условия осуществления которых определяются в соответствии с правилами информационной системы, отвечающей установленным законом признакам. Появление указанного закона было связано с попыткой регулирования криптовалют и цифровых активов и никак не связано с обеспечением гарантий основных прав человека в киберпространстве. Напротив, анализ правового регулирования интернета в России за последние 8 лет позволяет сделать вывод о значительном ограничении прав человека в онлайн-пространстве в отличии от тех же прав в оффлайне. Использование интернета само по себе, во многих случаях, является квалифицирующим признаком состава преступлений, за которые предусматривается более суровая ответственность.

Следует отметить, что резолюции ООН по цифровым правам не имеют обязательной юридической силы, и отдельные страны по-разному относятся к цифровым правам.

До настоящего времени единого международного договора, определяющего обязательный подход государства к регулированию цифровых прав в

[1] http://publication.pravo.gov.ru/Document/View/0001201903180027

киберпространстве, не существует. Наоборот, наметилось две основных тенденции «раскола» на коллегиальный (мультистейкхолдерный) подход правового регулирования интернета, которого придерживаются страны Европы и Америки, и подход, основанный на концепции цифрового суверенитета, поддерживаемый Россией, Ираном Китаем, странами азиатского и африканского региона. Разрозненность подходов и понимания, как должно происходить регулирование интернета и реализуемых в нем прав человека, приводит к кризису и невыполнению базовых норм международного права.

В настоящем докладе проведен обзор позитивных практик защиты «цифровых» прав. Целью доклада является исследование взаимосвязи «цифровых» прав с международным правом, возможностей защиты прав человека на основании норм международного и национального права и правоприменительной практики. Большое внимание уделяется нормам международного «мягкого» права, являющимся предпосылками и стимулом для развития внутренней политики государств в области регулирования интернета. Примеры норм национального законодательства разных стран позволяют оценить выполнение международных рекомендаций и соблюдение универсальных прав человека. Вопросы, являющиеся спорными или в недостаточной степени урегулированные нормами права, нередко становятся предметом исследования межгосударственных судебных органов. В завершение доклада приводятся выводы об основных тенденциях развития «цифровых» прав и регулирования сети интернет, а также даются рекомендации по совершенствованию российского законодательства в целях обеспечения цифровых прав человека.

СООТНОШЕНИЕ ЦИФРОВЫХ ПРАВ С ПРАВАМИ ЧЕЛОВЕКА

Развитие общественных отношений в XXI веке сопровождается проникновением современных цифровых технологий во все сферы деятельности социума: распространение информационных услуг создает базу становления цифровой экономики, происходит повсеместная сервизация экономических систем, цифровизация проникает в государственное управление и межличностные отношения. Внедрение компьютерных программ и электронных сервисов порождает новые возможности обработки данных, передачи информации, повышает скорость оказания услуг, их доступность, комфорт и удобство использования, экономит время и ресурсы.

Цифровизация становится возможной благодаря использованию глобальной сети интернет, как ключевого средства передачи информации между участниками отношений. Посредством сети интернет на общемировом уровне формируется «цифровая («виртуальная») среда жизнедеятельности» человека в которой он наделяется «цифровыми правами» по аналогии с реальной средой обитания.

Функционирование цифровой среды жизнедеятельности сопряжено с необходимостью индивидуализации каждого конкретного участника за счет сбора его персональных данных, данных о месте нахождения, предпочтениях, интересах, увлечениях, и любых других сведений, которые позволяют достичь заданных целей. Любая индивидуализация ведет к разной степени интенсивности проникновения в сферу личного, частного и семейного, обладающего для человека высшей ценностью.

Многочисленные нормы международного и национального законодательства позволяют защитить человека посредством закрепления его права на жизнь, на свободу и личную неприкосновенность, на неприкосновенность частной жизни (личную и семейную тайну), на свободу передвижения и выбора места пребывания и жительства, на свободу мысли и слова, свободу информации, право на участие в управлении делами государства, право на обращение в государственные органы и органы местного самоуправления[2].

Закономерным образом возникает необходимость гарантирования соблюдения универсальных прав человека при формировании новой сферы правового регулирования доступа к сети интернет и его использования, внедрения и

[2] См., например: Всеобщая декларация прав человека, принята Генеральной Ассамблеей ООН 10.12.1948 г.; Европейская конвенция по правам человека, принята Советом Европы в 1950 г., https://www.echr.coe.int/Documents/Convention_RUS.pdf; Конституция Российской Федерации, принята всенародным голосованием 12.12.1993 г.

использования современных цифровых технологий. Для этой цели выделяется отдельная группа «цифровых прав», которые представляют собой распространение универсальных прав человека на вновь возникающие потребности общества, основанные на цифровизации.

Как отмечают исследователи в области права, цифровые права человека - это конкретизация (посредством закона и правоприменительных, в том числе судебных, актов) универсальных прав человека, гарантированных международным правом и конституциями государств, применительно к потребностям человека и гражданина в обществе, основанном на информации. Задача государства признавать и защищать цифровые права граждан от всевозможных нарушений, обеспечивая при этом конституционно-правовую безопасность личности, общества и государства[3].

Среди «цифровых прав» обычно выделяют право на доступ к сети «Интернет» и цифровой телефонной связи, право на свободу выражения мнения и суждений, на свободу получения/распространения информации в сети «Интернет», право на конфиденциальность, анонимность, шифрование и обезличенность персональной информации. Наступление эры «цифровых прав» стало возможным благодаря распространению сети «Интернет» и цифровых технологий, с которыми «цифровые права» неразрывно связаны и за счет которых появились и реализуются.

Бурный рост цифровых технологий и их широкое распространение по всему миру стимулирует постоянное проведение исследований и осмысление происходящих новаций, определение их соотношения с существующей системой международного и национального права и выработку новых правовых теорий и рекомендаций. Являясь относительно новым явлением, институт «цифровых прав» находится в стадии становления, характеризуется неоднородностью и имеет свои особенности, определяемые на межгосударственном уровне и в каждом отдельно взятом государстве.

Унифицированию правового регулирования «цифровых прав» в значительной мере способствуют нормы международного права, вырабатываемые в результате информационного обмена о сложившихся практиках и многосторонних консультациях, организуемых международными организациями и инициативами с участием представителей государств. Традиционно нормы международного права делятся на нормы «мягкого» права (soft law), которые имеют рекомендательный характер и добровольно выполняются сторонами, и

---

[3] Егорова М.А., Блажеев В.В., Дюфло А., Андреева Л.В., Белицкая А.В., Белых В.С., Беляева О.А., Богданова Е.Е., Городов О.А., Гринь О.А., Трещакова Д., Ершова И.В., Ефремова Л.Г., Зенин С.С., Ючинсон К.С., Литвинова Н.Н., Мажорина М.В., Минбалеев А.В., Михеева И.Е., Петров Д.А., Попондопуло В.Ф., Решетникова С.Б., Самолысов П.В., Силина Е.В., Синюков В.Н., Ситник А.А., Фабрис Р., Хохлов Е.С., Цинделиани И.А. Цифровое право: учебник (под общ. ред. В.В. Блажеева, М.А. Егоровой). - М.: "Проспект", 2020. с. 64.

нормы «твердого» права (hard law), являющиеся обязательными и подлежащие имплементации в национальное законодательство[4].

Ввиду недавнего появления и сепарации «цифровых прав» возникает общественный запрос на выработку универсальных идей, принципов, рекомендаций, положений, которые помогут сформировать единые общемировые подходы к правовому регулированию в сфере цифровизации. Формирование таких подходов в значительной степени обеспечивается посредством международных норм «мягкого» права, которые государства еще не готовы принять в качестве обязательных к выполнению, но пределяющих ориентиры, задающих направление действия.

Межправительственные организации выполняют функции, связанные с укреплением законности, координацией политики и разработкой правовых норм в областях, касающихся безопасности, развития и управления, и во многих других[5]. Специальные докладчики ООН одними из первых начали уделять значительное внимание новым информационным технологиям, в особенности сети интернет, необходимости повсеместной организации доступа к нему не только в развитых, но и в развивающихся странах. Они указывали, что новые информационные технологии, в силу своей демократичности, могут обеспечить равные возможности для доступа к информационным ресурсам и помочь реализации права на свободу слова, предоставив каждому возможность активно участвовать в коммуникационном процессе[6]. Как отметил в своем докладе специальный докладчик ООН Амбеи Лигабо интернет, как и другие информационные и коммуникационные технологии, представляет беспрецедентную возможность донести информацию, мнения и идеи до людей, которые традиционно не охватывались средствами массовой информации»[7].

Благодаря Специальным докладчикам ООН, интернет получил признание по всему миру как важное средство реализации права на получение образования, борьбы с нетерпимостью посредством сообщений о взаимоуважении, распространяемых повсеместно, которое позволит собрать истинное множество голосов, звучащих на стольком количестве языков и отражающих такое количество культур, которое существует в мире. Запрет и чрезмерное регулирование доступа к сети интернет, как всего лишь еще одной форме

---

[4] См.: Лукашук И.И. Нормы международного права в международной нормативной системе. — М., 1997. С. 124.

[5] Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение. Совет по правам человека. A/72/350 https://www.un.org/ga/search/view_doc.asp?symbol=A/72/350&Lang=R

[6] Report of the Special Rapporteur to Commission on Human Rights resolution E/CN.4/1998/40 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G98/103/12/PDF/G9810312.pdf?OpenElement

[7] Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение. Совет по правам человека. A/HRC/7/14 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G08/112/12/PDF/G0811212.pdf?OpenElement

коммуникации, будет являться нарушением Всеобщей декларации прав человека, в частности, статьи 19[8].

Совет Европы в своих рекомендациях подчеркивает необходимость уважать, защищать и продвигать права человека и основные свободы в интернете. Государства должны создавать благоприятные условия для свободы интернета. С этой целью рекомендуется, чтобы государства проводили регулярные оценки среды свободы интернета на национальном уровне с целью обеспечения наличия необходимых правовых, экономических и политических условий для существования и развития свободы Интернета[9].

Интернет не должен быть сферой, полностью свободной от правового регулирования во избежание возможных угроз нарушения прав человека, в особенности потребителей и детей. Но необходимо избежать расширения оснований для обращения на новые технологии ограничительных мер, предусмотренных международными механизмами защиты прав человека[10]. Решение международного сообщества, отдельных государств и частного бизнеса инвестировать необходимые ресурсы в обеспечение доступа к сети интернет будет выглядеть бессмысленным в случае поддержки государствами политики и инициатив, направленных на ограничение доступа к информации[11]. Вызывают беспокойство те государства, в которых доступ к сети интернет предоставлен только высшим слоям общества, ограничен государственными фильтрами или лицензируется провайдерами, а в отдельных случаях и частными лицами[12].

Как отмечает Специальный докладчик ООН, интернет как возможное средство осуществления права на свободное выражение мнений будет соответствовать своему назначению при разработке государствами эффективной политики, направленной на обеспечение всеобщего доступа к Интернету, включающей конкретные планы действий[13].

---

[8] Report of the Special Rapporteur on the protection and promotion of the right to freedom of opinion and expression to Commission on Human Rights resolution E/CN.4/1999/64 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G99/107/66/PDF/G9910766.pdf?OpenElement

[9] Рекомендация CM / Rec (2016) 5 Комитета министров Совета Европы государствам-членам о свободе Интернета https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806415fa

[10] Report of the Special Rapporteur on the protection and promotion of the right to freedom of opinion and expression to Commission on Human Rights resolution E/CN.4/1999/64 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G99/107/66/PDF/G9910766.pdf?OpenElement

[11] Report of the Special Rapporteur on the protection and promotion of the right to freedom of opinion and expression to Commission on Human Rights resolution E/CN.4/2001/64 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G01/111/23/PDF/G0111123.pdf?OpenElement

[12] Report of the Special Rapporteur on the protection and promotion of the right to freedom of opinion and expression to Commission on Human Rights E/CN.4/2002/75 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G02/103/96/PDF/G0210396.pdf?OpenElement

[13] Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение. Совет по правам человека. A/HRC/17/27 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/132/03/PDF/G1113203.pdf?OpenElement

В целях достижения баланса возможностей доступа к сети интернет независимо от социального положения и уровня дохода, Программой развития ООН были организованы две инициативы, одна из которых – создание виртуальной библиотеки публикаций о добросовестном государственном управлении, документы которой доступны для бесплатного скачивания (http://magnet.undp.org), а вторая – создание сайта Программы развития ООН в Африке (https://www.africa.undp.org/) для обмена информацией, совместных идей и инициатив[14].

Немного позднее Совет Европы так же стал уделять особое внимание формированию рекомендаций по обеспечению признания и защиты «цифровых» прав, сходных с рекомендациями органов ООН[15].

Значительная роль в обеспечении соблюдения прав человека принадлежит международным неправительственным организациям, управляющим интернетом и созданным при поддержке ООН на основании четкого правозащитного подхода в целях долгосрочного развития сети интернет, создания, развития и использования совместных принципов, норм, правил, отражающих происходящую техническую эволюцию[16]. Такие организации, в том числе созданы, чтобы гарантировать совместное сосуществование в интернет-пространстве коммерческих инициатив, социальных и культурных проектов, которые поощряют свободные дебаты и диалоги, важные для построения лучшего мира на глобальном и локальном уровнях[17]. Многие международные организации играют определенную роль в процессах управления информационно-коммуникационными технологиями, поэтому важно, чтобы такие организации обеспечивали реальный публичный доступ к мерам политики, стандартам, докладам и иной информации относительно управления Интернетом, разработанным или подготовленным этими организациями и/или их членами, в том числе за счет облегчения доступа к бесплатным интерактивным ресурсам и общественно-просветительским инициативам[18].

Поддержка идеи неограниченного доступа к сети интернет по всему миру, независимо от социального статуса и материального положения, признание

---

[14] Report of the Special Rapporteur on the protection and promotion of the right to freedom of opinion and expression to Commission on Human Rights resolution E/CN.4/2001/64 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G01/111/23/PDF/G0111123.pdf?OpenElement

[15]Recommendations and declarations of the Committee od Ministers of the Council of Europe on the field of media and information society. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680645b44

[16] Моисеева М.Б., Дорофеев Д.Н., Матвеев М.С. «Роль международных и межправительственных организаций в процессе управления Интернетом». Проблемы современной науки и образования, 2018.

[17] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Human Rights Council. A/HRC/4/27
https://documents-dds-ny.un.org/doc/UNDOC/GEN/G07/101/81/PDF/G0710181.pdf?OpenElement

[18] Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение. Совет по правам человека. A/HRC/32/38 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/095/14/PDF/G1609514.pdf?OpenElement

возможности реализации в сети интернет права на свободу убеждений и свободное их выражение, права на информацию, способствует развитию и распространению глобальной сети интернет как независимой информационной площадки, что приводит к необходимости выработки международных и национальных принципов и правил ее использования.

НОРМЫ МЕЖДУНАРОДНОГО ПРАВА

Бурный рост цифровых коммуникационных технологий приводит к широкой доступности цифровых принимающих устройств, таких как интернет, мобильные смартфоны и устройства с поддержкой WiFi, 4G с помощью которых пользователи могут в режиме реального времени распространять, искать, получать информацию, в том числе излагать свои суждения, мнения, участвовать в дебатах и дискуссиях, получать и оказывать услуги с помощью интернет-сервисов. Происходит переход на следующую ступень интеграции глобальной сети в частную жизнь: цифровые принимающие устройства позволяют собирать большое количество данных о пользователях, включая их персональные данные, данные о перемещении, местонахождении, предпочтениях, хобби, увлечениях, пользовании сервисами, и др., обрабатывать, хранить и использовать их. Интернет становится одновременно общественным и личным пространством, которое вмешивается и влияет на реальную жизнь человека.

Возникает необходимость установить пределы такого вмешательства, которые позволят обеспечить соблюдение универсальных прав человека, защитить пользователей от возможных злоупотреблений со стороны тех, кто собирает, анализирует и использует их данные. Необходимо предоставить пользователю право на анонимность и конфиденциальность, право предоставлять свои данные по своему желанию. Именно поэтому Совет по правам человека и Генеральная Ассамблея ООН настоятельно призывают защищать права человека при использовании интернета, так же как они защищаются в обычной жизни[19]. А Совет Европы разработал руководство по правам человека для интернет-пользователей[20] и установил, что положения о правах и свободах, закрепленные в международных документах, применяются в равной степени как в режиме онлайн, так и в автономном режиме, а беспрепятственный трансграничный поток информации в сети интернет имеет решающее значение для полной реализации этих прав и свобод[21].

Беспокойство чрезмерным вмешательством в личную жизнь человека привело к возникновению соответствующих исследований, требований и положений в международных документах. Возникает необходимость выработки единых

---

[19] Записка Генерального секретаря. https://www.un.org/ga/search/view_doc.asp?symbol=A/71/373&Lang=R

[20] Руководство по правам человека для интернет-пользователей. Рекомендация CM/Rec(2014)6 принята Комитетом министров 16 апреля 2014 года и пояснительный меморандум. https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016804ccfa2

[21] Рекомендация CM / Rec (2015) 6 Комитета министров государствам-членам о свободном трансграничном потоке информации в Интернете https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f20

принципов и мер регулирования на международном уровне, с возложением на государства обязанностей по их имплементации в национальном законодательстве, а также установления гарантий их выполнения. Трансграничный характер цифровых прав позволяет руководствоваться универсальными принципами и нормами повсеместно, защитить цифровые права человека независимо от расы, цвета кожи, пола, языка, особенностей физического и психического развития, экономического происхождения или любого иного статуса.

В условиях повсеместной цифровизации, наибольшее внимание международное право уделяет защите свободы слова в сети интернет, защите частной жизни, личной и семейной тайны, анонимности и конфиденциальности, защите от слежения и от злоупотреблений частными компаниями.

ЗАЩИТА ДОСТУПА К ИНФОРМАЦИИ И СВОБОДЫ СЛОВА

Нормы международного «мягкого» права устанавливают обязанность государств принимать необходимые законодательные и административные меры в целях улучшения доступа к общественной информации для каждого человека в соответствии с существующими конкретными законодательными и процедурными нормами, которым должна соответствовать любая политика по обеспечению доступа к информации. Доступ к электронным средствам коммуникации рассматривается как необходимый элемент обеспечения развития и элемент социально-экономического права. В целях реализации данного права на равноправной основе, борьбы с нищетой и достижения целей в области развития, установленных в Декларации тысячелетия[22], государства должны взять на себя ответственность за облегчение и субсидирование доступа к электронным средствам коммуникации, гарантировать право на такой доступ и на свободу мнений и их свободное выражение[23]. Следует учитывать и укреплять преимущества Интернета, в частности тот его аспект, который позволяет даже индивидуальным пользователям распространять информацию в глобальном масштабе[24].

Наличие у граждан цифрового доступа является решающим для осуществления права на свободу мнений и их свободное выражение, однако нередко доступ ограничивается различными способами. В этой связи, Совет по правам человека в своей резолюции 32/13 недвусмысленно осудил меры по умышленному недопущению или нарушению доступа к информации или ее распространению в режиме онлайн в нарушение норм международного права прав человека и призвал все государства воздерживаться от таких мер и прекратить их использование[25]. Лишение пользователей доступа к сети интернет является чрезмерной мерой, и как следствие, нарушением пункта 3 статьи 19 Международного пакта о гражданских и политических правах. Во избежание таких мер, всем государствам следует разработать конкретную и

---

[22] Декларация тысячелетия ООН, принята резолюцией Генеральной Ассамблеи A/RES/55/2 https://undocs.org/ru/A/RES/55/2

[23] Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение Совет по правам человека A/HRC/14/23 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G10/130/51/PDF/G1013051.pdf?OpenElement

[24] Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение. Совет по правам человека. A/HRC/11/4 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G09/130/34/PDF/G0913034.pdf?OpenElement

[25] Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение. Совет по правам человека. A/HRC/35/22 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/077/50/PDF/G1707750.pdf?OpenElement

эффективную политику, чтобы позволить всем слоям общества на практике активно и недорого пользоваться интернетом[26].

Реализации права на доступ к информации в значительной мере способствует перевод веб-сайтов на различные языки, в том числе меньшинств и коренных народов, обеспечение их доступности для людей с ограниченными возможностями. На государства возлагается обязанность гарантировать наличие и доступность информации, касающейся государственного управления, в том числе на местном уровне, на языке всех граждан, интересы которых она затрагивает[27].

В статьях 19 Всеобщей декларации прав человека и Международного пакта о гражданских и политических правах[28] закреплено гарантированное право каждого выражать свое мнение, включая оскорбляющие, шокирующие или раздражающие взгляды, любым способом, в том числе посредством новых коммуникационных технологий, таких как интернет [29]. Изложенным онлайн высказываниям и информации должна предоставляться правовая защита, аналогичная защите убеждений и информации, изложенным иными способами, а выражения, зафиксированные онлайн, являются лишь одной из форм проявления свободы слова[30].

Благодаря низкой стоимости, децентрализованному характеру, широкому охвату и относительной анонимности в сети интернет появляются информационные площадки для распространения независимых мнений о государственных властях и политике. В результате государства начинают вводить ограничения, контроль, мониторинг, обработку и цензуру контента, распространяемого через интернет, блокировку интернет-ресурсов, содержащих политически некорректный контент, без каких-либо законных оснований или на основании широких и противоречивых законов, никак не обосновывая свои действия, или предоставляя обоснование, явно несоответствующее, непропорциональное заявленной цели[31]. В этой связи, Специальный докладчик ООН рекомендует государствам публиковать списки

---

[26] Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение. Совет по правам человека. A/HRC/17/27 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/132/03/PDF/G1113203.pdf?OpenElement

[27] Записка Генерального секретаря ООН A/66/290 https://documents-dds-ny.un.org/doc/UNDOC/GEN/N11/449/80/PDF/N1144980.pdf?OpenElement

[28] Международный пакт о гражданских и политических правах, принят резолюцией 2200 A (XXI) Генеральной Ассамблеи от 16.12.1966 г. https://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml

[29]Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение. Совет по правам человека. A/HRC/17/27 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/132/03/PDF/G1113203.pdf?OpenElement

[30] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression to Commission on Human Rights. E/CN.4/2000/63 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G00/102/59/PDF/G0010259.pdf?OpenElement

[31]Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение. Совет по правам человека. A/HRC/7/14 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G08/112/12/PDF/G0811212.pdf?OpenElement

блокируемых веб сайтов с подробным описанием и обоснованием необходимости блокирования каждого конкретного веб-сайта. Решение о блокировке контента должно приниматься судебным органом или иным независимым органом, который не находится ни под каким политическим, коммерческим или иным необоснованным влиянием, в соответствии с процессуальными гарантиями и критериями законности, необходимости и легитимности [32].

Ограничения права на свободу мнений и их свободное выражение чаще всего вводятся правительствами в качестве средства сдерживания критики и подавления инакомыслия, несмотря на то, что такие действия явно несовместимы с обязанностями государств, предусмотренными международным правом прав человека[33]. Наличие механизмов критики, в том числе политических лидеров, считается важным для того, чтобы отдельные лица отвечали за свои действия[34]. Поэтому любые законы, криминализующие или необоснованно ограничивающие свободу выражения мнений в интернете и за его пределами должны быть отменены. Государствам и неправительственным организациям следует воздерживаться от введения законов или правил, которые бы требовали «упреждающего» мониторинга или фильтрации контента[35].

В международных документах устанавливаются нормы «мягкого» права, определяющие основания ограничения или запрета доступа к информации, ограничения права на свободное выражение мнений, и носящие исключительный характер, направленные на недопустимость нарушения других прав и злоупотребления государствами мерами ограничения и ущемления в политических целях.

Специальные докладчики ООН отмечают, что ограничения или отказ в предоставлении информации должны всегда быть основаны на законе и носить временный характер. Ограничения или отказ в предоставлении информации должны быть изложены письменно с указанием оснований, а законодательством должен быть предусмотрена возможность обжалования такого ограничения или отказа в предоставлении информации[36]. Допустимые меры ограничения и ущемления прав должны представлять собой исключение из правил и сводиться до минимума, необходимого для достижения законной цели

---

[32] Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение. Совет по правам человека. A/HRC/17/27 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/132/03/PDF/G1113203.pdf?OpenElement

[33] См. там же.

[34] Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение. Совет по правам человека. A/HRC/11/4 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G09/130/34/PDF/G0913034.pdf?OpenElement

[35] Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение. Совет по правам человека. A/HRC/38/35 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/096/74/PDF/G1809674.pdf?OpenElement

[36] The right to freedom of opinion and expression. Report of the Special Rapporteur E/CN.4/2005/64* https://documents-dds-ny.un.org/doc/UNDOC/GEN/G05/106/90/PDF/G0510690.pdf?OpenElement

защиты других прав человека, предусмотренных Международным пактом о гражданских и политических правах или иными международными договорами в области прав человека.

Существующие международные стандарты в области прав человека, в частности пункт 3 статьи 19 Международного пакта о гражданских и политических правах, остаются ориентиром для определения видов ограничений, которые противоречат обязательствам государств гарантировать право на свободное выражение мнений. Любое ограничение права на свободное выражение мнений должно быть направлено, в первую очередь, на охрану прав других лиц, и соответствовать принципам законности, предсказуемости, транспарентности, необходимости и пропорциональности, иметь целью достижение защиты прав или репутации других лиц, охрану государственной безопасности[37]. Специальный докладчик ООН отмечает, что защита национальной безопасности или борьба с терроризмом не могут служить основаниями для ограничения права на свободное выражение мнений, за исключением случаев, когда выражение мнений имеет целью подстрекательство к насильственным действиям и может привести к таким насильственным действиям, а также имеется прямая и непосредственная связь между выражением мнений и вероятностью или возникновением таких насильственных действий[38]. Любое законодательство, ограничивающее право на свободное выражение мнений, должно применяться органом, который не находится ни под каким политическим, коммерческим или иным необоснованным влиянием, с предоставлением возможности опротестовать его противоправные действия и устранить их последствия.

Совет по правам человека в своей резолюции 12/16 заявил, что ограничения свободы выражения своего мнения не должны вводиться для защиты государства и его должностных лиц от высказывания суждений или критики со стороны общественности; на обсуждение проводимой правительством политики и политические дискуссии; представление докладов о правах человека, деятельности правительства и коррупции в органах власти; участие в избирательных кампаниях, мирных демонстрациях или политической деятельности, в том числе за мир и демократию; и выражение мнений, несогласия, религиозных взглядов или убеждений, в том числе лицами, принадлежащими к меньшинствам или уязвимым группам[39]. Никакой иск в порядке уголовного или гражданского судопроизводства за диффамацию в

---

[37] Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение Совет по правам человека A/HRC/14/23 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G10/130/51/PDF/G1013051.pdf?OpenElement

[38] Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение. Совет по правам человека. A/HRC/17/27 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/132/03/PDF/G1113203.pdf?OpenElement

[39] Резолюция Совета ООН по правам человека № 12/16 от 02.10.2009 г. http://cyberpeace.org.ua/files/ii_a_2.pdf

отношении гражданского служащего или выполнение им своих функций недопустим, а все законы, касающиеся неуважения властей, следует отменить.

Как отмечает Специальный докладчик ООН «произвольное использование уголовного законодательства с целью применения наказаний за законное выражение мнений является одной из наиболее пагубных форм ограничения этого права, поскольку оно не только создает сопутствующий негативный эффект, но и приводит к нарушениям других прав человека, таким как произвольное задержание и пытки и другие жестокие, бесчеловечные или унижающие достоинство виды обращения и наказания»[40]. Более того, Генеральный секретарь ООН просит государства немедленно отменить любой закон, который предусматривает несоразмерно жесткие санкции за выражение мнения, такие как смертная казнь. В связи с распространением призывов к ненависти в интернете государствам следует требовать удаления контента только через постановление суда, и посредники никогда не должны нести ответственность за тот контент, авторами которого они не являются[41].

[40] Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение. Совет по правам человека. A/HRC/17/27 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/132/03/PDF/G1113203.pdf?OpenElement

[41] Записка Генерального секретаря Поощрение и защита права на свободу мнений и их свободное выражение A/67/357 https://documents-dds-ny.un.org/doc/UNDOC/GEN/N12/501/27/PDF/N1250127.pdf?OpenElement

ЗАЩИТА ЧАСТНОЙ ЖИЗНИ

Нормами международного права гарантировано право на неприкосновенность частной жизни[42]. В статье 17 Международного пакта о гражданских и политических правах предусмотрено, что никто не может подвергаться произвольному или незаконному вмешательству в его личную и семейную жизнь, произвольным или незаконным посягательствам на неприкосновенность его жилища или тайну его корреспонденции или незаконным посягательствам на его честь и репутацию; каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств. В настоящее время термин «корреспонденция» охватывает все формы коммуникации, в том числе через интернет, а право на частную корреспонденцию подразумевает обязательства государства по обеспечению того, чтобы электронные письма и другие формы коммуникации в интернете доставлялись без вмешательства или контроля со стороны государственных органов или третьих сторон.

Помимо возможностей распространения и получения информации, интернет используется, в том числе, как средство наблюдения, помогающее выявить лиц, распространяющих информацию, установить их личность и местонахождение. В интернет попадает огромное количество личных данных, например, через веб-сайты социальных сетей. Хранение, использование и доступ к таким данным неопределенного круга лиц вызывает обеспокоенность с точки зрения соблюдения права на неприкосновенность частной жизни[43]. Широко используемый сбор «метаданных», может дать даже более полное представление о поведении человека, его социальных отношениях, личных предпочтениях и личности, чем то, что можно было бы узнать из самого содержания частного общения[44].

Навязчивый сбор данных и отслеживание движения нарушают неприкосновенность частной жизни и как следствие угрожают свободе слова постоянных пользователей интернета[45]. В докладе Управления Верховного комиссара ООН по правам человека признается, что любая регистрация данных коммуникации и даже сама возможность, что информация о

---

[42] Статья 12 Всеобщей декларации прав человека, принята Генеральной Ассамблеей ООН 10.12.1948 г.

[43] Записка Генерального секретаря ООН A/66/290 https://documents-dds-ny.un.org/doc/UNDOC/GEN/N11/449/80/PDF/N1144980.pdf?OpenElement

[44] Доклад Управления Верховного комиссара ООН по правам человека A/HRC/27/37 https://undocs.org/ru/A/HRC/27/37

[45] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Human Rights Council. A/HRC/4/27 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G07/101/81/PDF/G0710181.pdf?OpenElement

коммуникации может быть зарегистрирована, является потенциальным вмешательством в частную жизнь и что сбор и сохранение данных коммуникации является вмешательством в частную жизнь вне зависимости от того, принимаются ли во внимание или используются ли эти данные в дальнейшем[46].

Отдельные случаи вмешательства в частную жизнь, например, при запросах о предоставлении данных о пользователях и хранение таких данных третьей стороной, могут иметь сдерживающее воздействие на выражение мнений. В таком случае, государствам следует обеспечивать, чтобы наблюдение было санкционировано судебным органом, удостоверяющим, что запрос необходим и соразмерен заявленным государством целям[47].

В этой связи, особой формой соблюдения права на неприкосновенность частной жизни является защита личных данных, которая должна производиться посредством соответствующего закона. Во исполнение пункта 2 статьи 17 Международного пакта о гражданских и политических правах, через законы о защите данных государства должны регулировать запись, обработку, использование и передачу личных данных через автоматизированные системы, права на сообщение, изменение и, в случае необходимости, удаление данных, а также защищать затрагиваемых лиц от злоупотреблений со стороны государственных органов и частных сторон и устанавливать эффективные меры контроля.

Специальный докладчик отмечает, что применение ограничений или оговорок в отношении права на неприкосновенность частной жизни возможно лишь в исключительных случаях, таких как меры государственного контроля с целью отправления уголовного правосудия, предупреждения преступления или борьбы с терроризмом, при условии соответствия таких мер критериям допустимых ограничений. При этом такие исключительные случаи не могут являться произвольными, а именно непропорциональными конечной цели, необоснованными в конкретных обстоятельствах или незаконными. В первую очередь, условия ограничения права людей на неприкосновенность частной жизни должны быть установлены законом, который соответствует положениям, целям и задачам Международного пакта о гражданских и политических правах, а реализация таких ограничений допустима исключительно на основании специального решения, вынесенного уполномоченным государственным органом, как правило, судебным[48]. Таким образом, вмешательство, допустимое

---

[46] См. там же.

[47] Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение. Совет по правам человека. A/HRC/35/22 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/077/50/PDF/G1707750.pdf?OpenElement

[48] Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение. Совет по правам человека. A/HRC/17/27 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/132/03/PDF/G1113203.pdf?OpenElement

по национальным законам, может является "незаконным", если национальное право вступает в противоречие с положениями упомянутого Пакта.

Устанавливаемые законом ограничения права на неприкосновенность частной жизни, должны основываться на принципах законности, необходимости и соразмерности, должны соответствовать другим правам человека, быть доступными для ознакомления, четкими и однозначными, во избежание различных толкований и не единообразного правоприменения.

Законом должны, в том числе, предусматриваться эффективные и доступные средства правовой защиты. Обязанность государства по защите включает принятие надлежащих мер для предупреждения и расследования нарушений прав человека, совершаемых третьими лицами, наказания за них и возмещения ущерба[49]. Пунктами 3 a) и b) статьи 2 Международного пакта о гражданских и политических правах предусмотрено обязательство государств предоставлять жертвам нарушений доступ к эффективным средствам правовой защиты, жалобы на такие нарушения должны рассматриваться компетентными судебными, административными или законодательными органами или любым другим компетентным органом, который предусмотрен правовой системой государства. Правоохранительные органы и органы прокуратуры должны незамедлительно, тщательно и эффективно проводить расследования по заявлениям о нарушениях, при необходимости предоставляя защиту физическим лицам от действий организаций частного сектора[50].

Дополнительным средством защиты может служить право на предъявление индивидуальных исков как к государственным, так и к негосударственным субъектам. Для этого необходимо закрепить в национальном законодательстве правила, касающиеся юрисдикции, доказательств, соблюдения сроков и других основных пороговых условий, например, определить основания для возбуждения исков против частных субъектов, обеспечить, чтобы суды могли принимать и рассматривать в качестве доказательств результаты криминалистической экспертизы технических экспертов[51].

---

[49] Руководящие принципы предпринимательской деятельности в аспекте прав человека: Осуществление рамок Организации Объединенных Наций в отношении «защиты, соблюдения и средств правовой защиты» HR/PUB/11/04 https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_ru.pdf

[50] Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение. Совет по правам человека. A/HRC/41/35 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/148/78/PDF/G1914878.pdf?OpenElement

[51] См. там же.

ЗАЩИТА АНОНИМНОСТИ, ШИФРОВАНИЯ И КОНФИДЕНЦИАЛЬНОСТИ

Возможность использования сети «Интернет» позволяет многим людям участвовать в обсуждениях острых тем общественной жизни анонимно, без раскрытия своей настоящей личности, например, благодаря использованию псевдонимов на форумах и в чатах, что в значительной степени благоприятствует свободе выражения собственного мнения. Как отмечает Генеральный секретарь ООН, необходимо гарантировать каждому право на анонимное самовыражение в «Интернете»[52]. Специальный докладчик ООН призывает все страны обеспечить каждому человеку возможность выражать свое мнение в Интернете анонимно, и не вводить системы регистрации подлинных имен[53]. В свою очередь, государствам рекомендуется поощрять безопасность и конфиденциальность в онлайновой среде путем информирования общественности, а также поощрять применение надежных средств шифрования и анонимизации.

Шифрование и анонимность, а также лежащая в их основе концепция обеспечения безопасности являются залогом конфиденциальности и безопасности, необходимых для осуществления права на свободу мнений и их свободное выражение в цифровой век. В условиях отсутствия такой безопасности порою невозможно осуществлять другие права, включая экономические права, права на неприкосновенность частной жизни и право на жизнь и физическую неприкосновенность.

С учетом важного значения шифрования и анонимности с точки зрения осуществления права на свободу мнений и их свободное выражение, права на неприкосновенность частной жизни, ограничения, вводимые в их отношении, должны строго подчиняться принципам законности, необходимости, соразмерности и правомерности их цели. В законе за частными лицами должно признаваться право соблюдать конфиденциальность своих цифровых сообщений с помощью технологий и средств шифрования, позволяющих им сохранить анонимность в онлайновой среде. Для защиты правозащитников и журналистов, следует предусмотреть положения, предусматривающие доступ к технологиям по обеспечению безопасности сообщений и меры по содействию их применения.

---

[52] Записка Генерального секретаря Поощрение и защита права на свободу мнений и их свободное выражение A/67/357 https://documents-dds-ny.un.org/doc/UNDOC/GEN/N12/501/27/PDF/N1250127.pdf?OpenElement

[53] Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение. Совет по правам человека. A/HRC/17/27 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/132/03/PDF/G1113203.pdf?OpenElement

Государствам рекомендуется отказаться от любых мер, снижающих степень безопасности частных лиц в онлайновой среде, а также воздержаться от введения требований, при которых обязательным условием для доступа к электронным сообщениям или онлайновым услугам являлась бы идентификация пользователей или которые предусматривали бы регистрацию сим-карты владельцев мобильных телефонов. Расшифровка должна быть санкционирована судом в соответствии с нормами внутреннего законодательства и международного права, опирающимися на доступные для всеобщего ознакомления законы, и применяться исключительно на адресной и индивидуальной основе в отношении отдельных лиц (а не совокупности пользователей) при условии защиты прав лиц на надлежащее судопроизводство.

Специальный докладчик ООН рекомендует корпоративным субъектам пересмотреть свою практику на предмет ее соответствия правозащитным нормам. Компаниям следует воздерживаться от блокирования или ограничения передачи зашифрованных сообщений и разрешать анонимные виды общения. Следует уделять внимание усилиям по расширению доступности ссылок на центры обработки зашифрованных данных, содействию использованию в веб-сайтах надежных технологий и повсеместному введению устанавливаемого по умолчанию сквозного шифрования[54].

[54] Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение. Совет по правам человека. A/HRC/29/32 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/87/PDF/G1509587.pdf?OpenElement

ЗАЩИТА ОТ СЛЕЖЕНИЯ

В цифровую эпоху коммуникационные технологии также расширили возможности правительств, компаний и отдельных лиц осуществлять слежение, перехват и сбор данных, а технологические платформы подвержены массовому электронному слежению. В настоящее время государство обладает большими, чем когда-либо, возможностями осуществления одновременного, интрузивного, адресного или широкомасштабного слежения[55].

В результате отсутствия развитой нормативно-правовой базы, достаточного национального законодательства, правоприменительной практики, процедурных гарантий и эффективного надзора, незаконное цифровое слежение приводит к отсутствию ответственности за произвольное или незаконное вмешательство в личную жизнь [56]. В резолюции Генеральной Ассамблеи о Праве на неприкосновенность частной жизни в цифровую эпоху, отмечается необходимость уважать и защищать право на неприкосновенность личной жизни в контексте цифровой коммуникации, а те права, которые человек имеет в оффлайновой среде, должны также защищаться и в онлайновой среде. Слежение за цифровыми сообщениями, их перехват и сбор персональных данных, включая массовое слежение, должно осуществляться с соблюдением международных обязательств в области прав человека и соответствующих правовых рамок, которые должны быть доступными для общественности, ясными, точными, всеобъемлющими и недискриминационными[57]. Законодательство должно предусматривать, что слежение государством за сообщениями должно осуществляться в исключительных случаях и под надзором независимого судебного органа. В законе должны быть четко прописаны гарантии, касающиеся характера, охвата и продолжительности возможных мер слежения, оснований, требующихся для их применения, органов власти, уполномоченных санкционировать, осуществлять такие меры и надзирать за ними, и типа средств правовой защиты, предусмотренных национальным законодательством. Должно предусматриваться право частных лиц знать о том, что их сообщения отслеживались или что к их коммуникационным данным получило доступ

[55] Доклад Управления Верховного комиссара ООН по правам человека A/HRC/27/37 https://undocs.org/ru/A/HRC/27/37

[56] См. там же.

[57] Право на неприкосновенность частной жизни в цифровую эпоху. Резолюция Генеральной Ассамблеи от 17.12.2018 г. https://undocs.org/ru/A/RES/73/179

государство, направление уведомления об этом возможно сразу же после окончания слежения[58].

Международные нормы накладывают на государства, применяющие средства слежения, обязательства обеспечить соответствие практики слежения национальным нормам, которые, в свою очередь, должны отвечать стандартам международного права. Для соответствия стандартам национальное законодательство должно предусматривать возможность использования технологий слежения только в соответствии с правозащитными стандартами законности, необходимости и обоснованности целей, а также правовые механизмы возмещения ущерба[59].

Международный пакт о гражданских и политических правах[60] и Всеобщая декларация прав человека защищают права каждого человека на неприкосновенность частной жизни, свободу мнений и их свободное выражение[61]. В соответствии со статьей 2 Пакта, каждое государство-участник обязано уважать и обеспечивать всем находящимся в пределах его территории и под его юрисдикцией лицам права, признаваемые в настоящем Пакте. Государства также обязаны защищать отдельных лиц от вмешательства третьих сторон, однако неясно, обеспечивают ли государства в целом позитивную правовую защиту от целенаправленного слежения, например, по аналогии с транснациональным слежением. Одним из способов защиты могли бы стать комиссии по установлению истины для оказания помощи жертвам цифрового слежения представлять показания и которые изучали бы вопросы причастности корпораций к цифровым нарушениям[62].

В качестве отдельных рекомендаций по предотвращению несанкционированного слежения Специальный докладчик ООН отмечает необходимость установления общественного надзора, консультаций и контроля за закупками государством технологий слежения. Учреждение рабочей группы по правам человека позволило бы предлагать и рассматривать стандарты экспорта, учитывающие правозащитные аспекты при передаче технологий, достигать транспарентности путем разработки четких и осуществимых руководящих принципов межправительственного обмена информацией и

---

[58] Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение. Совет по правам человека. A/HRC/23/40 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G13/133/05/PDF/G1313305.pdf?OpenElement

[59] Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение. Совет по правам человека. A/HRC/41/35 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/148/78/PDF/G1914878.pdf?OpenElement

[60] Международный пакт о гражданских и политических правах, принят резолюцией 2200 A (XXI) Генеральной Ассамблеи от 16.12.1966 г. https://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml

[61] См. пункт 1 статьи 17 Пакта, которая повторяет статью 12 Декларации: «никто не может подвергаться произвольному или незаконному вмешательству в его личную и семейную жизнь, произвольным или незаконным посягательствам на неприкосновенность его жилища или тайну его корреспонденции».

[62] Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение. Совет по правам человека. A/HRC/41/35 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/148/78/PDF/G1914878.pdf?OpenElement

публичного раскрытия информации, касающихся стандартов лицензирования, решений о выдаче, изменении или отклонении лицензий, случаев или схем неправомерного использования технологий слежения и соответствующих нарушений прав человека, а также режима обращения с цифровыми уязвимостями.

До установления режима гарантий, предусматривающий защиту прав человека, государствам следует незамедлительно ввести мораторий на экспорт, продажу, передачу, использование или обслуживание разработанных частным образом средств слежения. В случае экспорта технологий слежения, следует обеспечить учет мнения общественности, проведение многосторонних консультации при рассмотрении заявок на получение экспортных лицензий, а также максимальный доступ к соответствующим материалам[63].

Любые методики и практика слежения, применяющиеся вне правового поля, должны быть поставлены под законодательный контроль. Государства должны криминализировать незаконное слежение с государственными или частными субъектами. Такие законы не должны использоваться для борьбы с разоблачителями или другими частными лицами, стремящимися предать гласности нарушения прав человека. Они также не должны препятствовать законному надзору за деятельностью правительства со стороны граждан.

Меры по слежению за сообщениями должны быть предписаны законом и удовлетворять нормам ясности и четкости, быть строго и очевидно необходимыми для достижения законной цели и соответствовать принципу соразмерности. Любое вмешательство в осуществление права на неприкосновенность личной жизни, семейной жизни, жилища или тайны переписки должно санкционироваться законом, который доступен для всеобщего ознакомления; обеспечивает соответствие сбора, доступа или использования содержащихся в сообщениях данных конкретным предусмотренным в законе целям; достаточно четко определяющим условия, при которых такое вмешательство допускается, порядок получения разрешения, категории лиц, в отношении которых может вестись слежение, предельные сроки слежения; порядок использования и хранения полученных данных; предусматривающим эффективные гарантии против злоупотребления[64].

Предоставление коммуникационных данных государствам должно контролироваться независимым органом, таким как суд или надзорный механизм, способный обеспечить транспарентность и подотчетность практики слежения государства за сообщениями. Персональная информация не должна собираться и храниться исключительно в целях слежения, при этом любые коммуникационные данные, собираемые корпоративными субъектами в ходе

---

[63] См. там же.

[64] Доклад Управления Верховного комиссара ООН по правам человека A/HRC/27/37 https://undocs.org/ru/A/HRC/27/37

оказания коммуникационных услуг, должны соответствовать наивысшим стандартам защиты данных.

Специальный докладчик рекомендует государствам проявлять полную транспарентность в отношении применения и охвата методов и полномочий слежения, для чего, необходимо публиковать как минимум обобщенную информацию о количестве одобренных и отклоненных запросов, данные о запросах в разбивке по провайдерам услуг, расследованиям и целям; предоставлять частным лицам информацию о законах, разрешающих слежение за сообщениями и их применении; разрешить провайдерам услуг публикацию информации о применяемых ими процедурах при слежении государства за сообщениями, соблюдении ими этих процедур и отчетов о слежении государства за сообщениями[65].

[65] Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение. Совет по правам человека. A/HRC/23/40 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G13/133/05/PDF/G1313305.pdf?OpenElement

ЗАЩИТА ИНФОРМАЦИОННЫХ ПОСРЕДНИКОВ

Любая коммуникация в сети интернет происходит при участии серии посредников, например, интернет-провайдеров, социальных сетей, поисковых систем, которые осуществляют техническую поддержку и содержательное наполнение интернет-сервисов. Во многих государствах на законодательном уровне закреплена ответственность посредников за отсутствие блокировки или удаление незаконного контента посредством прямых норм или через защиту частной жизни и данных. В случае отказа провайдеров онлайн-платформ от контроля пользователей и размещаемого ими контента, они могут быть привлечены к ответственности, включая потерю права заниматься предпринимательской деятельностью.

Возложение на посредников обязательств и привлечение их к ответственности приводит к контролю контента, распространяемого или создаваемого пользователями, а также к частной цензуре в целях самозащиты. В конечном итоге, ответственность посредников влияет на права пользователей, включая права на свободу выражения мнений, свободу информации и неприкосновенность частной жизни, личную и семейную тайну.

В целях изменения губительной практики, Специальный докладчик ООН отмечает, что полномочия по применению цензуры никогда не должны передаваться частному субъекту и что ни одно лицо не должно нести ответственность за размещение в интернете контента, автором которого оно не является, посредники не должны нести ответственность за отказ от принятия мер, нарушающих права человека, тем более в виде таких несоразмерных санкций, как большие штрафы или тюремное заключение. Государства должны воздерживаться от возложения на посредников обязательств по рассмотрению вопросов контента, поскольку такое делегирование закрепляет примат корпоративных решений над ценностями прав человека[66].

Любые запросы о блокировании доступа к определенному контенту или о раскрытии личной информации в строго ограниченных целях должны направляться посредникам на основании решения суда или иного независимого компетентного органа. Государствам надлежит публиковать подробные отчеты о направлении посредникам требований, связанных с контентом, и привлекать общественность к участию в обсуждении вопросов регулирования.

---

[66] Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение. Совет по правам человека. A/HRC/38/35 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/096/74/PDF/G1809674.pdf?OpenElement

Посредникам надлежит открыто сообщать соответствующему пользователю и, при необходимости, широкой общественности о применении ограничительных мер и распространять эти ограничения исключительно на соответствующий контент. При этом затрагиваемые пользователи должны иметь доступ к средствам защиты, например, возможность обжалования принятого решения[67].

По инициативе мирового гражданского сообщества был выработан список рекомендаций по ограничению ответственности посредников за передаваемую ими информацию с целью поощрения свободы слова и инноваций, составленный на международных инструментах обеспечения прав человека и других международных стандартах[68]. Согласно указанному списку, посредники должны быть освобождены от ответственности за информацию третьих лиц, в том числе за хостинг незаконной информации третьих лиц; требование по ограничению доступа к информации должно быть основано на решении независимого и беспристрастного судебного органа; запрос на ограничение доступа к информации должен быть четким, недвусмысленным и следовать должной процедуре; законы и правила по ограничению доступа и практика их применения должны соответствовать критериям необходимости и пропорциональности, устанавливать процедуру, с возможностью обжаловать решение об ограничении доступа; законы, правила и практики по ограничению доступа к информации должны быть прозрачными и подотчетными.

Имплементация в национальном законодательстве вышеизложенных принципов, выработанных группами гражданского общества и экспертами со всего мира посредством открытого, совместного обсуждения, будет способствовать повышению уровня доверия к государственной власти, инновационному развитию и соблюдению международных стандартов в области прав человека. Согласие в имплементации единых принципов по всему миру будет способствовать единообразию законов и правоприменительной практики, соответствовать безграничной природе интернета и международной роли посредников.

Посредники, которые обеспечивают доступ пользователей к сети интернет, обладают широкими возможностями по обеспечению реализации универсальных прав человека. В случаях, когда государства требуют участия компаний в применении цензуры или наблюдения, компании должны стремиться к предотвращению или смягчению негативных последствий такого участия для прав человека, стремиться не вызывать нарушения прав человека, не становиться их соучастниками и не способствовать им. В случае выстраивания договоренностей с корпоративными партнерами, компаниям необходимо отдавать приоритет выполнению своих правозащитных обязанностей и

---

[67] Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение. Совет по правам человека. A/HRC/17/27 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/132/03/PDF/G1113203.pdf?OpenElement

[68] Манильские принципы ответственности посредников от 24.03.2015 г. https://www.eff.org/files/2015/07/01/manila_principles_1.0_ru.pdf

стремиться к укреплению уже существующих деловых отношений в целях предотвращения или смягчения негативных последствий для прав человека[69].

Разработка общепринятого глобального стандарта обеспечения свободы выражения мнений на интернет-платформах по всему миру, строгая оценка разработки продуктов, текущий анализ и пересмотр осуществляемых операций, а также конструктивные консультации с общественностью и гражданским обществом, во избежание тайных договоренностей с государствами о стандартах контента и их применении, будут помогать воплощению прав человека[70]. В идеальном гражданском обществе, посредники должны вести открытую деятельность и быть подотчетными обществу, когда одной из первоочередных задач выступает создание механизмов подотчетности в масштабах всей индустрии (как, например, совета социальных сетей)[71]. Относительно технологий слежения, компании должны немедленно прекратить продажу, передачу и поддержку таких технологий в случае отсутствия убедительных доказательств принятия достаточных мер в вопросах должной осмотрительности, транспарентности и подотчетности, с тем чтобы предотвратить или смягчить последствия использования технологий слежения с нарушением прав человека[72].

Происходящее в последние годы развертывание систем искусственного интеллекта также возлагает на государства и компании ряд обязательств, в первую очередь, по уважению прав человека применительно ко всем приложениям искусственного интеллекта. Компаниям следует придерживаться транспарентности и подотчетности о сферах и способах использования технологий искусственного интеллекта и автоматизированных методов. Проведение публичных консультаций и поддержка общественности будут способствовать успешному внедрению новых продуктов или служб, а аудиторские проверки системы искусственного интеллекта могут значительно повысить уровень доверия, так же как система рассмотрения жалоб

---

[69] Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение. Совет по правам человека. A/HRC/35/22 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/077/50/PDF/G1707750.pdf?OpenElement

[70] См. в том числе Руководящие принципы предпринимательской деятельности в аспекте прав человека: Осуществление рамок Организации Объединенных Наций в отношении «защиты, соблюдения и средств правовой защиты» HR/PUB/11/04 https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_ru.pdf

[71] Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение. Совет по правам человека. A/HRC/38/35 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/096/74/PDF/G1809674.pdf?OpenElement

[72] Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение. Совет по правам человека. A/HRC/41/35 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/148/78/PDF/G1914878.pdf?OpenElement

пользователей на решения, принятые системами искусственного интеллекта, и оперативного их рассмотрения[73].

[73] Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение. Генеральная Ассамблея. A/73/348 https://www.un.org/ga/search/view_doc.asp?symbol=A/73/348&Lang=R

НОРМЫ НАЦИОНАЛЬНОГО ПРАВА

Нормы международного права устанавливают универсальные рекомендации, правила и принципы, которыми должны руководствоваться государства при выработке политики и законов, регулирующих цифровые права граждан. Полноту и степень имплементации международных норм во внутреннее законодательство определяет каждое государство самостоятельно.

Российская Федерация в полной мере признала закрепленные в международных нормах права человека только после распада СССР: Всеобщая декларация прав человека была опубликована только в 1988 году[74]. Международный пакт об экономических, социальных и культурных правах и Международный пакт о гражданских и политических правах СССР ратифицировал в 1973 году, а вступили Пакты в силу для СССР в 1976 году.

Впоследствии в Конституции Российской Федерации были закреплены все общепризнанные права и свободы человека. В частности, в статье 23 признано право каждого на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени, закреплено право на тайну переписки, телефонных переговоров, почтовых, и иных сообщений, а ограничение этого права допускается только на основании судебного решения. В статье 24 запрещается сбор, хранение, использование и распространение информации о частной жизни лица без его согласия. В статье 27 закреплено право каждого свободно передвигаться, выбирать место пребывания и жительства. Статьей 29 каждому гарантируется свобода мысли и слова, право каждого на свободу информации; гарантируется свобода массовой информации, цензура запрещается. В части 4 статьи 15 Конституции предусмотрен приоритет международного права, а в статье 46 каждому гарантируется судебная защита его прав и свобод (возможность отстаивать права в суде).

Первые попытки осмысления роли новых информационных технологий и создания единого информационного пространства начались еще в 90-х годах. Так был принят ряд концепций, наиболее значимой из которых стала «Концепция формирования информационного общества в России», согласно которой России необходимо интегрироваться в мировое информационное пространство, для этого на государство возлагалась обязанность обеспечивать право населения на доступ к информации и информационным ресурсам,

[74] Большая Российская энциклопедия. https://bigenc.ru/law/text/3474878

гарантировалась свобода слова и возможность диалога граждан и власти с помощью информационного общества[75].

Новый этап развития правовых отношений, связанных с законодательной реализацией цифровых прав, основанных на закрепленных в Конституции правах человека, связан с принятием Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Указанные законодательные акты позволили Российской Федерации выполнить ряд международных обязательств, возникших в связи с цифровизацией. В частности, Закон «Об информации, информационных технологиях и о защите информации»: 1) определил правовой режим информации в сети «Интернет» и закрепил право на доступ к информации в сети «Интернет»; 2) определил основания для ограничения доступа к информации, в сети «Интернет»; 3) установил общедоступность и бесплатность информации о деятельности государственных органов и органов местного самоуправления, размещенной в информационно-телекоммуникационных сетях; 4) ввел обязанность защиты информации; 5) предусмотрел ответственность в сфере информации, информационных технологий и защиты информации. Положения указанного закона конкретизируются и подкрепляются подзаконными актами, определяющими взаимодействие распространителей информации с Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций[76], устанавливающими методики подсчета пользователей[77], требования по защите информации[78], порядок идентификации информационных ресурсов, и другими положениями, принятыми для реализации закона[79].

Закон «О персональных данных» позволил: 1) признать значимость идентификации личности, в том числе, в сети интернет посредством характеризующей ее информации и необходимость защиты прав и свобод

---

[75] Концепция формирования информационного общества в России, одобрена решением Государственной комиссии по информатизации при Государственном комитете РФ по связи и информатизации от 28.05.1999 № 32; http://www.iis.ru/library/riss/

[76]См., например, приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.12.2016 № 306 «Об утверждении Порядка функционирования системы взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с владельцами новостных агрегаторов»; и др.

[77]Например, приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.12.2016 № 307 "Об утверждении Методики определения количества пользователей программ для электронных вычислительных машин, сайтов и (или) страниц сайтов в сети интернет, которые используются для обработки и распространения новостной информации в сети интернет в сутки"

[78]Например, Приказ Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"

[79]Например, приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 11.02.2019 № 21 "Об утверждении Порядка идентификации информационных ресурсов в целях принятия мер по ограничению доступа к информационным ресурсам"

человека и гражданина при обработке персональных данных; 2) предусмотреть обязательное согласие личности на обработку персональных данных и право на отзыв такого согласия; 3) установить общие правила конфиденциальности и запрета на передачу персональных данных третьим лицам; 4) установить требования к сбору персональных данных, их безопасности; 5) определить государственный орган по защите прав субъектов персональных данных[80].

В целях конкретизации и обеспечения применения положений закона, были приняты нормативные правовые акты, устанавливающие требования к защите и безопасности персональных данных[81], а также предусматривающие организацию и осуществление государственного контроля и надзора в сфере обращения с персональными данными[82].

Среди действующих законов также необходимо отметить закон, который получил название «право на забвение», который является имплементацией прецедентного права Европейского суда справедливости по делу Гонсалес VS Испания. Он устанавливает, что с 1 января 2016 г. поисковики в сети интернет обязаны удалять из поисковой выдачи ссылки на «недостоверную», «распространяемую с нарушением законодательства» и неактуальную информацию о гражданах по их требованию[83]. Однако конструкция описанной нормы в российском законодательстве, при полном отсутствии разъяснений практики Верховным и Конституционным судом, вызывает множество коллизий при правоприменении, на которые указывают правозащитные организации[84].

Выполнение Российской Федерацией международных рекомендаций по обеспечению доступа пользователей к электронным средствам коммуникации и электронным сервисам обеспечивается, в значительной мере, посредством реализации государственных программ, таких как «Информационное общество» и «Цифровая экономика». Данные программы направлены на: 1) ускоренное внедрение цифровых технологий в экономике и социальной сфере; 2) обеспечение населения и социально значимых организаций качественным доступом в интернет; 3) создание сети беспроводной связи и подключение к сети интернет социально значимых объектов; 4) предоставление гражданам и

---

[80]См. постановление Правительства РФ от 16.03.2009 № 228 "О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций"

[81]См., например, постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"; постановление Правительства РФ от 06.07.2008 № 512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных"; и др.

[82]См. постановление Правительства РФ от 13.02.2019 № 146 "Об утверждении Правил организации и осуществления государственного контроля и надзора за обработкой персональных данных".

[83] Федеральный закон от 13.07.2015 № 264-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и статьи 29 и 402 Гражданского процессуального кодекса Российской Федерации» / Официальной сайт Президента России. http://kremlin.ru/acts/bank/39945

[84] Конституционный суд не против «права быть забытым», https://roskomsvoboda.org/46672/

организациям доступа к приоритетным государственным услугам и сервисам в цифровом виде, создание национальной системы управления данными, развитие инфраструктуры электронного правительства; 5) повышение удобства использования гражданами, организациями и органами государственной власти и органами местного самоуправления государственных (муниципальных) информационных систем и сервисов; и др.[85]

Несмотря на значительный прогресс в области обеспечения базового доступа в интернет, внедрения цифровых сервисов и предоставления множества государственных услуг в электронном виде, необходимо отметить создание в России собственной модели контроля за информацией, применения технологий слежения и цензуры, которые порождают неблагоприятную атмосферу и препятствуют инновационному развитию, ограничивая при этом права на шифрование, анонимность, доступ и получение информации.

Ежегодно расширяются основания для блокировки сайтов и появляются новые органы, имеющие полномочия на принятие решений о внесудебном ограничении доступа к сайтам и веб-сервисам в сети интернет. Одним из наиболее спорных и не транспарентных законов, устанавливающих порядок ограничения доступа к информации в сети интернет стал Федеральный закон № 398-ФЗ от 28 декабря 2013 года (известный также как "закон Лугового"). Согласно решению ЕСПЧ по делу Kablis v Russia блокировка аккаунта до вынесения судебного решения о незаконности опубликованного контента является незаконной. В ходе рассмотрения дела Европейский суд также пришел к следующим выводам:

- в «процедуре блокировки, предусмотренной разделом 15.3 закона, отсутствуют необходимые гарантии против злоупотреблений, в частности жесткий контроль над масштабом блокирования и эффективный судебный контроль;
- ст. 15.3 закона об информации является неопределенной, а ее «авторитетное толкование» Верховным или Конституционным судами отсутствует;
- Генпрокуратуре предоставлено слишком широкое усмотрение «как в отношении оснований для блокировки, так и в отношении ее масштаба»;
- стандарты, применяемые национальными судами РФ, «не соответствовали принципам, закрепленным ст. 10 Конвенции»: суды не должны подходить к таким делам формально, а обязаны изучить вопрос о «необходимости блокирования рассматриваемых публикаций в демократическом обществе с учетом фактов и обстоятельств дела».

---

[85] См. подробнее постановление Правительства РФ от 15.04.2014 № 313 "Об утверждении государственной программы Российской Федерации "Информационное общество". Распоряжение Правительства Российской Федерации от 28.07.2017 № 1632-р об утверждении программы «Цифровая экономика Российской Федерации»; Паспорт национальной программы "Цифровая экономика Российской Федерации", утвержден президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам 24.12.2018 № 16.

В целом российское интернет-пространство за последние 8 лет стало чрезмерно «зарегулированным» благодаря, в том числе, принятым в 2016 году Доктрине информационной безопасности[86], множеству поправок в Федеральный закон об информации №149-ФЗ, а также "закону Яровой", который установил: обязанность хранения пользовательского трафика на территории России до полугода (переговоров, текстовых сообщений, и др.); уголовную ответственность за призывы к террористической деятельности, публичное оправдание терроризма или его пропаганду, совершенные с использованием сети интернет; административную ответственность с высокими штрафами за отказ посредников передавать правоохранительным органам информацию о пользователях сети интернет, включая их голосовые сообщения, переписку, изображения, а также за отказ предоставить информацию, необходимую для декодирования электронных сообщений[87].

В продолжение Доктрины информационной безопасности, принятой еще в декабре 2016 года, Президент России в мае 2017 года подписал разработанную Советом безопасности РФ «Стратегию развития информационного общества на 2017-2030 годы»[88]. В п.34 документа указано, что для развития сети интернет и информационной инфраструктуры РФ необходимо проводить мероприятия на международном уровне, в том числе «создать новые механизмы партнерства, призванные с участием всех институтов общества выработать систему доверия в сети интернет, гарантирующую конфиденциальность и личную безопасность пользователей, конфиденциальность их информации и исключающую анонимность, безответственность пользователей и безнаказанность правонарушителей в сети интернет». В контексте принятой стратегии, анонимность рассматривается как порок сетевых коммуникаций, позволяющий преступникам и правонарушителям уходить от установленной законом ответственности, но не как эффективное средство защиты приватности и реализации права на свободу слова.

---

[86] Доктрина информационной безопасности, утверждена указом Президента РФ от 05.12.2016 № 646 https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html

[87] Федеральный закон от 06.07.2016 № 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" Федеральный закон от 06.07.2016 № 375-ФЗ; "О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности". http://www.pravo.gov.ru, 07.07.2016

[88] Указ Президента Российской Федерации от 09.05.2017 № 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы" http://publication.pravo.gov.ru/Document/View/0001201705100002?index=0&rangeSize=1

В 2017 году вступил в силу закон, позволяющий также ограничивать доступ к VPN-сервисам, анонимайзерам и операторам поисковых систем[89], А в 2018 году Таганский суд Москвы вынес решение о блокировке мессенджера Telegram в связи с отказом передать правоохранительным органам информацию для дешифровки сообщений пользователей[90]. Применение указанного закона в совокупности с другими нормами (например, "закона Лугового"[91]) привело к фактическому ограничению прав российских пользователей на использование сервисов, предоставляющих возможность сквозного шифрования, в том числе мессенджеров Blackberry, IMO, Line, VChat, и почтовых сервисов Startmail, Protonmail, Tutanota.

С 01 января 2018 г. вступили в силу поправки к закону «Об информации», предусматривающие обязательную идентификацию пользователей мессенджеров по абонентскому номеру через оператора связи. За отказ от исполнения закона предусматриваются штрафы для юридических лиц до 1 млн руб. Помимо этого оператор связи сможет по решению Роскомнадзора заблокировать доступ к мессенджеру.

Силовые структуры Российской Федерации продолжают настаивать на необходимости полной деанонимизации пользователей интернета и ограничению возможностей не сертифицированных ФСБ алгоритмов стойкого шифрования.

Наибольшее количество беспокойства вызывает так называемый закон о «суверенном интернете», который предусматривает установку всеми операторами в стране специального оборудования (DPI), предоставленного Роскомнадзором, с помощью которого российские власти смогут отслеживать пользовательский трафик, а также и ограничивать доступ к веб-сайтам и целым мобильным приложениям из списка Роскомнадзора. К 2021 году должна быть создана национальная система доменных имен[92].

Существенные ограничения цифровых прав российских пользователей в связи с принятием и применением новых законов в РФ ведет их в международные суды, в том числе ЕСПЧ в поисках эффективных мер защиты нарушенных прав. В настоящее время в производстве ЕСПЧ находится 5 жалоб из России по блокировкам, объединенных в одно производство[93], порядка 30 жалоб по делу

---

[89] Федеральный закон от 29 июля 2017 года № 276-ФЗ «О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации"» http://www.pravo.gov.ru, 07.07.2016

[90] Решение Таганского суда Москвы по делу № 2-1779/2018 от 13.04.2018 https://www.mos-gorsud.ru/rs/taganskij/services/cases/civil/details/2cc72aea-39e7-4f8e-adc9-37d170966efa

[91] https://ru.wikipedia.org/wiki/%D0%A4%D0%B5%D0%B4%D0%B5%D1%80%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D0%B7%D0%B0%D0%BA%D0%BE%D0%BD_%E2%84%96_398-%D0%A4%D0%97_%D0%BE%D1%82_28_%D0%B4%D0%B5%D0%BA%D0%B0%D0%B1%D1%80%D1%8F_2013_%D0%B3%D0%BE%D0%B4%D0%B0

[92] Принят закон о «суверенном интернете» http://duma.gov.ru/news/44551/

[93] ЕСПЧ приступил к рассмотрению жалоб на блокировки сайтов в России https://roskomsvoboda.org/32025/

Telegram,[94] а также множество жалоб, связанных с привлечением пользователей к уголовной ответственности за публикацию постов в социальных сетях.

Однако длительное неисполнение Российской Федерацией решений ЕСПЧ, в том числе по делу Захаров против России[95], Каблис против России[96] в части изменения национальных законов, регулирующих цифровые права и вопросы слежки, демонстрирует явное нежелание российских властей менять текущее законодательство.

Для того, чтобы Россия имела возможность не выполнять решения межгосударственных судебных органов, в 2015 году были приняты поправки в Федеральный конституционный закон 21.07.1994 № 1-ФКЗ «О Конституционном Суде Российской Федерации», согласно которым, Конституционный Суд Российской Федерации разрешает вопрос о возможности исполнения решения межгосударственного органа по защите прав и свобод человека[97].

Указанные акты свидетельствуют о постоянном росте использования технологий слежения, ограничения доступа к интернет-ресурсам, искоренении анонимности и шифрования, запуске неизбирательного контроля и самоцензуры. С принятием закона о необязательности выполнения решений Европейского суда по правам человека, граждане России были ограничены в возможности применения одного из наиболее эффективных средств защиты нарушенных прав. В результате Российская Федерация не выполняет в должной мере возложенные на нее международные обязательства и все в большей степени ущемляет «цифровые права» граждан, что, в результате, негативно сказывается на реализации конституционных и международных прав человека.

Сходную политику ограничений «цифровых» прав реализует Китайская Народная Республика, в качестве обоснования указывая на необходимость обеспечения информационной безопасности в стране. Запрету подлежит любая информация, подрывающая государственную власть и расшатывающая социальную стабильность. Министерство государственной безопасности вправе заблокировать любой интернет-ресурс, вредящий репутации государства. Согласно правилам для интернет-провайдеров, перед получением лицензии провайдер, услуги которого касаются одной из социально значимых сфер, обязан получить согласие и одобрение определенных наблюдательных советов. На провайдеров возлагается обязанность создавать механизмы фильтрации контента, мониторинга активности пользователей и направлять соответствующую информацию государственным органам. Провайдеры также должны вести полный учет появляющихся на сайте информации и комментариев, фиксировать время публикации, регистрационные

---

[94] Битва за Telegram переносится в Страсбург https://roskomsvoboda.org/47943/

[95] https://hudoc.echr.coe.int/fre?i=001-159324

[96] https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-192769%22]}

[97] Федеральный конституционный закон от 14.12.2015 № 7-ФКЗ "О внесении изменений в Федеральный конституционный закон "О Конституционном Суде Российской Федерации" http://www.consultant.ru/

имена пользователей, а с 2015 года при регистрации на сайте запрашивать у пользователя подтверждение его личности. В качестве меры наказания в 2013 году была введена уголовная ответственность за распространение в интернете клеветы и ложных слухов, порочащих репутацию, в случае, если эту информацию прочитали более 5 тысяч пользователей или сделали ее «репост» более 500 раз[98].

Законодательство и правоприменительная практика в разных юрисдикциях отличается неоднородностью и разнообразием. Так, в странах Европы реализуется противоположный подход к правовому регулированию интернета. В Европейской Союзе при участии 36 гражданских и правозащитных организаций, действующих в 21 стране Европейского Союза, разработана Хартия цифровых прав, основанная на Хартии Европейского союза об Основных правах, и имеющая основной целью защитить фундаментальные права и свободы человека в «цифровой среде» жизнедеятельности. В Хартии цифровых прав содержатся руководящие положения, которые необходимо поддержать кандидатам в Европейский Парламент, направленные на обеспечение правомерного доступа к сети интернет и онлайн-сервисам, защиту информации, шифрования, анонимности и конфиденциальности, защиту от всеохватывающего и бесконтрольного слежения, контроль экспорта технологий слежения и цензуры, поддержку бесплатного, открытого, демократического и коллегиального (multi-stakeholder) подхода координации интернет-ресурсов и стандартов[99].

В Европейском Союзе действуют пять директив, принятых в 2002 году и составляющих существующую нормативно-правовую базу для сетей и услуг электронных коммуникаций Директива о доступе 2002/19/ЕС, Директива об авторизации 2002/20/ЕС, Рамочная директива 2002/21/ЕС об общей нормативно-правовой базе для сетей и услуг электронных коммуникаций, Директива об универсальном обслуживании 2002/22/ЕС и Директива о конфиденциальности и электронных коммуникациях 2002/58/ЕС. Директивы способствуют одновременному созданию единого европейского информационного пространства и инклюзивного информационного общества. На основании указанных директив все государства-члены Европейского Союза должны обеспечить каждому подключение к сети общего пользования в фиксированном месте и по доступной цене с помощью как минимум одного провайдера, при этом, предоставляемое соединение должно поддерживать передачу голоса, факсимильной связи и данных со скоростями передачи данных, достаточными для обеспечения функционального доступа в сеть интернет, соединения для передачи данных должны обеспечивать передачу данных со скоростью, достаточной для доступа к онлайн-услугам.

---

[98] Глазунов О.Н., Авдеенко В.В. Специфика правового регулирования сети интернет в Китайской Народной Республике https://cyberleninka.ru/article/n/spetsifika-pravovogo-regulirovaniya-seti-internet-v-kitayskoy-narodnoy-respublike/viewer

[99] Хартия цифровых прав https://edri.org/wp-content/uploads/2014/06/EDRi_DigitalRightsCharter_web.pdf

Обеспечению европейцев доступом к скоростному интернет во многом способствует реализация Цифровой повестки Плана действий Европы, которая среди приоритетных направлений деятельности выделяет создание цифрового рынка; повышение интернет-доверия и безопасности, гарантируя предоставление более быстрого доступа в интернет; повышение цифровой грамотности, навыков и интеграции; поощрение инвестиций в исследования и разработки; и др.[100].

Среди основных положений директив, способствующих соблюдению «цифровых» прав, необходимо отметить право конечных пользователей решать, какой контент они хотят отправлять и получать и какие услуги, приложения, аппаратное и программное обеспечение они хотят использовать для таких целей; право на получение информации об использовании их личной информации в каталогах подписчиков и право не включать свои данные в общедоступный каталог подписчиков. На государства-члены возложена обязанность уважать основные права граждан, в том числе в отношении конфиденциальности и соблюдении процедур защиты прав. Директива о конфиденциальности и электронных коммуникациях предписывает обязанность обеспечения соответствия включения данных конечных пользователей в базы данных установленным гарантиям защиты персональных данных, а также предусматривает гармонизацию законов государств-членов, чтобы потребители и пользователи имели одинаковый уровень защиты конфиденциальности и персональных данных, независимо от технологии, используемой для предоставления конкретной услуги.

В целях предоставления консультаций потребителям и надлежащего учета интересов граждан государства-члены должны создать соответствующий механизм консультаций. Компетентные национальные органы государств-членов должны защищать интересы граждан, в частности, способствуя обеспечению высокого уровня защиты персональных данных и конфиденциальности. На посредников возлагается обязанность осуществлять соответствующие технические и организационные меры защиты в области обработки персональных данных, например, от их потери, а также учет нарушений в области обработки персональных данных, чтобы обеспечить возможность дальнейшего анализа и оценки компетентными национальными органами. В случае нарушения правил обращения с персональными данными компетентные национальные органы и пользователи, чьи данные и конфиденциальность могут пострадать от нарушения должны быть уведомлены. Уведомление должно содержать информацию о мерах, принятых провайдером для устранения нарушения, а также рекомендации для соответствующего пользователя.

---

[100] См. подробнее: Цифровая Повестка Европы. Ключевые инициативы. https://ec.europa.eu/commission/presscorner/detail/en/MEMO_10_200

Директивами закреплено право пользователей получать четкую и исчерпывающую информацию о тех действиях, которые могут привести к хранению информации об оборудовании пользователя или получению доступа к уже сохраненной информации для любых целей, начиная от законных (таких как определенные типы файлов cookie) и заканчивая необоснованным вторжением в частную сферу (таких как шпионское ПО или вирусы). Пользователи имеют право на отказ от предоставления информации или участия в определенных действиях, при этом способы реализации права на отказ должны быть максимально удобными. В свою очередь согласие пользователя на обработку данных может быть выражено с использованием соответствующих настроек браузера или другого приложения. Европейским законодательством гарантируется защита от вторжения в личную жизнь пользователей посредством нежелательных сообщений в целях прямого маркетинга с помощью электронной почты, SMS, MMS и других аналогичных приложений[101].

Государства-члены Европейского Союза принимают национальные законы, способствующие реализации директив. В статье 5A Конституции Греции закреплено право каждого участвовать в Информационном Сообществе, а на государство возлагается обязанность оказания содействия в доступе к информации, передаваемой в электронном виде[102]. В 2000 году парламент Эстонии принял закон, устанавливающий доступ к интернету в качестве одного из основных прав человека[103], а в 2009 году Конституционный Совет во Франции провозгласил свободу доступа к услугам общественных сетевых коммуникаций («public online communication services»), принимая во внимание важность реализации права на свободное выражение идей и мнений[104].

В статье 52 Закона Испании № 2/2011 от 04.03.2011 «Об устойчивой экономике» предусмотрена обязанность Правительства создать с помощью любой технологии условия для предоставления услуги подключения населения к сети связи общего пользования с функциональной пропускной способностью доступа в интернет, под которой понимается широкополосная передача данных со скоростью 100 мегабит в секунду[105].

Финляндия стала первой страной, взявшей на себя обязательство по обеспечению всего населения страны доступом к широкополосным каналам

---

[101] См. подробнее: Директива ЕС 2009/136/ЕС https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?id=556364

[102] Конституция Греции http://www.hellenicparliament.gr/UserFiles/f3c70a23-7696-49db-9148-f24dce6a27c8/001-156%20aggliko.pdf

[103] Colin Woodard, "Estonia, where being wired is a human right", Christian Science Monitor, 1 July 2003.

[104] См. Решение Конституционного Совета Франции 2009-580 от 10.07.2009 https://www.conseil-constitutionnel.fr/sites/default/files/as/root/bank_mm/anglais/2009_580dc.pdf

[105] Закон Испании № 2/2011 от 04.03.2011 «Об устойчивой экономике» https://www.boe.es/diario_boe/txt.php?id=BOE-A-2011-4117

связи в соответствии с Законом о рынке связи[106], и предоставила каждому гражданину право на доступ к недорогому и высококачественному соединению с нисходящим тарифом на уровне минимум 1 мегабит в секунду[107]. В 2014 году в Финляндии был принят Кодекс Цифрового Общества, установивший «приемлемость» платы за соединение, запрет на ограничение использования сети интернет, кроме прямо предусмотренных в законе случаев; предусмотревший конфиденциальность переписки; возможность обработки и передачи данных о местонахождении при условии уведомления и согласия лица, данные о местоположении которого обрабатываются или передаются; процедуру ограничения доступа к материалам, нарушающим права третьих лиц, с обязательным уведомлением пользователя, разместившего материалы и предоставления ему возможности защитить свои права; установивший строгие ограничения прямого маркетинга [108].

С 01 января 2020 в штате Калифорния по аналогии с Европой вступил в силу собственный прогрессивный закон о защите прав приватности потребителей (California Consumer Privacy Act), который определил, что персональные данные – это любые данные, по которым можно идентифицировать человека, например, биометрия, геолокация, история активности в интернете, информация о трудоустройстве или образовании. В законе закреплено право интернет-пользователя потребовать у организации информацию, которую она о нем собрала, и список третьих лиц, которым она стала известна (право доступа), а также информацию о целях сбора персональных данных и их источниках; пользователю предоставлено право отказаться от передачи своих персональных данных третьим лицам и потребовать удалить информацию о себе с серверов компании и серверов третьих лиц[109].

Примером положительного опыта защиты прав граждан при использовании сети интернет является закон о принципах, гарантиях, правах и обязанностях использования интернета в Бразилии, известный как "marco civil". Данным законом устанавливается широкий перечень гарантий и прав пользователей, в частности, использование сети интернет в Бразилии основано на уважении права на свободу выражения мнений, признании всемирного масштаба сети интернет, открытости и сотрудничестве; закреплено право каждого на доступ к сети интернет, к информации, знаниям и участию в культурной жизни. Законом устанавливаются принципы защиты конфиденциальности, защиты персональных данных, сохранения и гарантии сетевого нейтралитета, сохранение стабильности, безопасности и функциональности сети. Ответственность за

---

[106] См. Раздел 60C Закона о рынке связи https://www.finlex.fi/en/laki/kaannokset/2003/en20030393.pdf

[107] Стефани Борг Псаила. Управление Интернетом. https://www.diplomacy.edu/blog/right-access-internet-countries-and-laws-proclaim-it

[108] Разделы 110, 112, 136, 138, 160-162, 189-192, 201-204 Кодекса Цифрового Общества (917/2014) https://www.finlex.fi/en/laki/kaannokset/2014/en20140917.pdf

[109]California Consumer Privacy Act of 2018 http://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180AB375

непринятие мер по удалению контента, признанного несоответствующим закону, назначается только на основании судебного решения. Закон предусматривает защиту прав пользователей на неприкосновенность частной жизни, а в случае нарушения данного права, возмещение материального и морального ущерба, тайну корреспонденции, конфиденциальность, а также защиту персональных данных. Для передачи данных пользователей третьим лицам, сбора, использования, хранения и обработки персональных данных, необходимо свободное, явное и осознанное согласие. Данные пользователя должны быть удалены по его запросу. Содержание переписки пользователей может быть предоставлено третьим лицам только по решению суда.

Важным новшеством является правило сетевого нейтралитета («net neutrality»), закрепленное в статье 9 закона и согласно которому, провайдеры телекоммуникационных услуг обязаны обрабатывать любые передаваемые данные одинаково, независимо от их содержания, происхождения и назначения, оказываемым услугам, используемым терминалам или приложениям. При предоставлении подключения к Интернету, независимо от его стоимости, а также при передаче, коммутации или маршрутизации данных, запрещается блокировать, отслеживать, фильтровать или анализировать содержимое передаваемых данных[110].

Индия также признала принцип сетевого нейтралитета в качестве одного из основополагающих, гарантируя пользователям открытый и честный интернет. Данный принцип подразумевает одинаковое отношение интернет-провайдеров к любому контенту, не отдавая предпочтение или отказывая в доступе к определенным веб-сайтам, услугам или приложениям. Новые положения индийских законов указывают на недопустимость дискриминации и вмешательства в обработку контента, а именно, блокирование, пренебрежение, замедление или предоставление льготных скоростей или обработки определённому контенту. В случае нарушения правил, провайдеры могут лишиться лицензии и права работать в пределах индийских границ[111].

В отличие от Индии и Бразилии, в Соединенных Штатах Америки широко обсуждается отмена принципа сетевого нейтралитета, хотя отдельные штаты, такие как Калифорния, Нью-Джерси, Вашингтон и Орегон, закрепили принцип в своем законодательстве. Кроме того, Сенат США выносил на голосование вопрос отмены мер защиты конфиденциальности в интернете, а администрация Трампа выразила поддержку такой инициативы[112].

---

[110] Marco Civil da Internet LEI Nº 12.965, DE 23 DE ABRIL DE 2014 https://www2.camara.leg.br/legin/fed/lei/2014/lei-12965-23-abril-2014-778630-norma-pl.html

[111] Rishi Iyengar «India now has the 'world's strongest' net neutrality rules» https://money.cnn.com/2018/07/12/technology/india-net-neutrality-rules-telecom/index.html

[112] Seth Fiegerman «Net neutrality rules are now repealed: What it means» https://money.cnn.com/2018/06/11/technology/net-neutrality-repeal-explained/?iid=EL; Seth Fiegerman «Congress just killed your Internet privacy protections» https://money.cnn.com/2017/03/28/technology/house-internet-privacy-repeal/?iid=EL

В целях защиты персональных данных в Европейском Союзе был принят ряд документов, а именно, Общие положения о защите данных (GDPR), Правоохранительная Директива по защите данных и Регламент защиты данных для органов и учреждений Европейского Союза[113]. Введенные нормы устанавливают обязательное наличие легальных оснований для сбора и использования данных; ограничение целью, когда обработка должна сводиться к тому, что было заявлено субъекту данных, а конкретные задачи должны быть закреплены в политике приватности и чётко соблюдаться; правило минимизации данных, когда для достижения поставленной цели используется минимально возможное количество данных; ограниченный срок хранения данных, которые должны быть удалены если в них больше нет необходимости; обязательное хранение данных в безопасном месте; ответственность за обработку персональных данных, назначение ответственного за защиту данных лица; и др. Совершенствование и гармонизация правового регулирования по защите данных способствовала более активному использованию прав гражданами, которые начали совершать больше покупок онлайн и чаще запрашивать государственные органы по защите данных о предоставлении информации и направлять жалобы. Физические лица также чаще начали отзывать свое согласие на обработку персональных данных и использовать право отказаться от коммерческой коммуникации[114].

В Индии был разработан Закон о защите личных данных, сходный по своему правовому регулированию с европейским законодательством. Закон предусматривает право владельцев персональных данных знать об обработке персональных данных; право изменять персональные данные, если они некорректны или устарели; право требовать предоставить свои данные в электронном формате; право на ограничение публичности или прекращение использования персональных данных[115].

В отличие от европейских Общих положений о защите данных, предусматривающих требование получить согласие на обработку персональных данных, в Калифорнии организация должна обрабатывать запросы пользователей. В случае если организация неправомерно

---

[113] General Data Protection Regulation 2016/679 and repealing Directive 95/46/EC https://eurlex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679; Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32016L0680; Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC: https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A32018R1725

[114] См. Коммуникация: правила защиты данных как средство обеспечения доверия в ЕС и за его пределами – подведение итогов (COM /2019/374) https://ec.europa.eu/info/sites/info/files/aid_development_cooperation_fundamental_rights/aid_and_development_by_topic/documents/communication_2019374_final.pdf

[115] The Personal Data Protection Bill https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf

использовала персональные данные или отказалась ответить на запросы, пользователь, права которого нарушены, имеет право подать на организацию в суд. За несоблюдение сроков рассмотрения жалобы о нарушении, связанном с персональными данными, и непринятие мер в течение месяца организации грозит штраф. Если в организацию не поступал запрос, самостоятельно раскрывать сведения о нарушениях она не обязана. Однако, если данные пользователя были потеряны или украдены, законодательством предусмотрен штраф в размере от 100 до 750 долларов каждому пользователю[116].

Положительным примером защиты граждан от незаконного слежения и обработки цифровых отпечатков лица без согласия человека может служить закон Калифорнии, признающий технологии распознавания лиц несущими значительную угрозу гражданским правам и свободам. Общий калифорнийский закон был принят после того как Сан-Франциско, Окленд, Кембридж, Беркли и Сомервилл запретили применение технологии в своих городах. Распознавание лиц и другие технологии биометрической слежки приравниваются к обязанности граждан показать удостоверение личности с фотографией бесчисленное количество раз, они также позволяют следить за людьми без их согласия. Поэтому законом устанавливается запрет на установку, активацию и использование таких технологий применительно к камерам должностных лиц или собираемых ими данных. В случае нарушения данного запрета, пострадавший имеет право подать иск к нарушителю с требованием возмещения причиненного вреда[117].

В связи с широким использованием технологий слежения правоохранительными органами в США и необходимостью общественного надзора, консультаций и контроля в данной сфере, в ряде общин были созданы гражданские советы по надзору для регулирования использования и закупок таких технологий. Например, город Окленд в штате Калифорния принял постановление, содержащее ряд требований к процессу закупки технологий слежения, таких как 1) процесс одобрения, осуществляемый соответствующими ведомствами; 2) информирование общественности о таких закупках; 3) периодическое информирование общественности о выдаче таких разрешений, закупках и случаях использования технологий слежения[118].

Различается правовое регулирование блокировки незаконного контента и ответственности и роли посредников в этом процессе. Некоторые государства пытаются защитить посредников: например, в соответствии с директивой ЕС об

---

[116] ИТ-ГРАД Американский аналог GDPR: что нужно знать об акте CCPA https://habr.com/ru/company/it-grad/blog/422979/

[117] Assembly bill 1215, approved by Governor, 8 October, 2019. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1215

[118] См. American Civil Liberties Union of Northern Calofornia, «Oakland Becomes Latest Municipality to Reclaim Local Control Over Surveillance Technologies Used By Local Law Enforcement», 2 May 2018. https://www.aclunc.org/news/oakland-becomes-latest-municipality-reclaim-local-control-over-surveillance-technologies-used

электронной коммерции провайдер услуг хостинга для создаваемого пользователями контента может освобождаться от ответственности за незаконный контент, если он не знает об осуществлении незаконной деятельности, или, если он незамедлительно удаляет соответствующий контент после того, как узнает о нем[119], а в США Закон о защите авторских прав в цифровое тысячелетие (DMCA) предоставляет посредникам средства защиты, если они удаляют соответствующий контент сразу же после получения уведомления[120]. В Чили и в Бразилии закон не требует от посредников предупреждения или блокирования доступа к пользовательскому контенту, нарушающему законы об авторских правах, до тех пор, пока не будет принято соответствующее судебное постановление[121].

В Республике Корея государство перестало использовать посредников для применения цензуры от его имени или принуждать их к этому после учреждения Корейской комиссии по стандартам связи – квазигосударственной и квазичастной структуры, ответственной за регулирование контента в сети интернет[122].

В Австралии по общему правилу запрещен перехват телекоммуникации или доступ, без предварительного уведомления отправителя и получателя, о сохраненных телекоммуникациях каким-либо физическим или юридическим лицом, за исключением случаев, таких как установка или обслуживание телекоммуникационного оборудования. Доступ к сообщениям может быть получен правоохранительными органами на основании ордера «на телекоммуникационные услуги» (для перехвата в реальном времени) или ордера на «хранящиеся средства коммуникации» (на сохраненные сообщения без требования об уведомлении авторов сообщения), контролируемых генеральным прокурором. Для осуществления наблюдения правоохранительные органы должны получить ордер «для устройств наблюдения»[123].

До 2015 года в Австралии интернет-провайдеры не были обязаны сохранять личные данные пользователей, но согласно судебному приказу должны были оказывать «необходимую помощь» любому федеральному, штатному или территориальному правоохранительному органу в рамках уголовного

---

[119] Директива об электронной коммерции, 2000/31/EC, статья 14. http://base.garant.ru/2568904/

[120] Закон о защите авторских прав в цифровое тысячелетие, статья 512. https://www.congress.gov/bill/105th-congress/house-bill/2281/text/enr

[121] Ley No. 20435, Modifica La Ley No.17.336 Sobre Propiedad Intelectual, chap. III, art. 85-L – art. 85-U, adopted on 4 May 2010. https://www.wipo.int/edocs/lexdocs/laws/es/cl/cl051es.pdf Marco Civil da Internet LEI Nº 12.965, DE 23 DE ABRIL DE 2014 https://www2.camara.leg.br/legin/fed/lei/2014/lei-12965-23-abril-2014-778630-norma-pl.html

[122] Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение. Совет по правам человека. A/HRC/17/27 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/132/03/PDF/G1113203.pdf?OpenElement

[123] Australia and New Zealand. https://opennet.net/research/regions/australia-and-new-zealand

расследования. В 2015 году в Австралии был принят закон о хранении данных, согласно которому австралийские телекоммуникационные компании должны хранить большие объемы метаданных в течение двух лет. Закон охватывает данные о том, кто кому звонил или отправлял сообщения, и в течение какого времени, а также о местонахождении, объеме передаваемых данных, информации об используемом устройстве и всех без исключения IP-данных электронной почты. При этом, хранению подлежат именно метаданные, а не содержание звонков и сообщений, как это предусмотрено законодательством РФ. Австралийские интернет-провайдеры обязаны хранить подробные записи почти всего, касающегося электронной почты или чата (кроме их реального содержимого), однако для таких сервисов как Gmail, Hotmail, Facebook и Skype сделано исключение.

В Австралии до сих пор основным законом, предусматривающим защиту конфиденциальности, является Закон о конфиденциальности 1988 года, предусматривающий основную законодательную базу для защиты частной жизни (включая защиту данных в Интернете). Закон о конфиденциальности - это прежде всего основанная на принципах основа, которая применяется к сбору, использованию, хранению и уничтожению «личной информации». Основными принципами закона являются: «законные и справедливые способы сбора данных»; оператор, осуществляющий сбор, должен «принять разумные меры», чтобы гарантировать, что субъект, чья личная информация собирается, знает оператора и как с ним связаться», может получить доступ к собранной информации, знает цели, для которых собирается информация, уведомлен об организации, которой информация может быть раскрыта; оператор, осуществляющий сбор, не должен использовать или раскрывать личную информацию субъекта данных для целей, отличных от основной цели сбора, а также обязан «принять разумные меры для обеспечения того, чтобы личная информация, которую он собирает, использует или раскрывает, была точной, полной и актуальной», обязан защищать ее от неправомерного использования, потери и несанкционированного доступа, изменения или раскрытия. По результатам достижения цели, личная информация должна быть уничтожена или удалена. Функции надзора и рассмотрения жалоб выполняются независимым уполномоченным по вопросам конфиденциальности.

В 2011 году профильный комитет Сената Австралии выражал обеспокоенность по поводу адекватности существующей системы защиты конфиденциальности в интернете, в связи с чем периодически высказываются предложения о введении новшеств, которые смогли бы учесть современные тенденции «цифровизации» общества[124].

В отличие от нормативного регулирования Австралии, в парламент Новой Зеландии в марте 2020 года был внесен новый законопроект о

[124]Online Privacy Law: Australia https://www.loc.gov/law/help/online-privacy-law/2012/australia.php

конфиденциальности, позволяющий актуализировать устаревший закон 1993 года, поскольку за прошедшие годы распространение интернета оказало значительное влияние на бизнес, правительство и использование личной информации. Основными новшествами являются: в случае если оператору стало известно о нарушении конфиденциальности, он обязан уведомить пострадавших лиц и Уполномоченного по вопросам конфиденциальности; принятие обязательных к исполнению решений по жалобам на доступ к информации возложено на Уполномоченного по вопросам конфиденциальности; обязательное принятие операторами разумных мер для обеспечения защиты личной информации, отправляемой за рубеж, в соответствии с приемлемыми стандартами конфиденциальности; вводится новый вид правонарушения, который предусматривает ответственность до 10 000 долларов за введение в заблуждение оператора, повлекшее изменение чужой информации или уничтожение документов по запросу; Уполномоченный по вопросам конфиденциальности вправе сократить сроки расследования нарушений[125].

[125] Privacy https://www.justice.govt.nz/justice-sector-policy/key-initiatives/privacy/

ПРИМЕРЫ КЛЮЧЕВЫХ СУДЕБНЫХ ДЕЛ

Законодательство, регулирующее цифровые права, неоднократно становилось предметом исследования судов различных юрисдикций. Одним из наиболее значимых дел стало решение Европейского суда справедливости о признании недействительным соглашения «Безопасная гавань» между Европейским союзом и США, на основании которого происходила массовая передача личных данных европейских граждан в США такими компаниями как Google и Facebook. Как установил суд, Агентство национальной безопасности США получало массовый доступ к переданным данным, защита данных не была обеспечена надлежащим образом, а пользователи могли подвергаться слежению. Хранение данных происходило независимо от того, удалил их пользователь из сети или нет. По результатам вынесенного решения многие компании будут обязаны пересмотреть свои политики обработки персональных данных в целях соблюдения прав пользователей и предоставления им права на возмещение причиненного вреда в соответствие с требованиями директив и регламентов Европейского союза[126]. Следующим шагом стало признание Европейским судом справедливости права национальных органов по защите персональных данных предъявлять требования к организации, управляющей сервисом на национальном языке и представляющей интересы головного офиса, базирующегося за рубежом[127]. До вынесения указанного решения, такие компании как Facebook, выбравшие штаб-квартирой своей деятельности в Европе Ирландию, подпадали под юрисдикцию только выбранной страны и могли вести деятельность в любом государстве-члене Европейского союза без получения дополнительного одобрения контрольных органов в каждой из стран.

Интересную позицию высказал Европейский суд справедливости, признав администратора группы в Facebook совместно с самой социальной сетью субъектом, контролирующим обрабатываемые данные посетителей страницы и ответственным за их обработку[128]. В другом деле владелец сайта Fashion ID и Facebook признаны совместными операторами обработки (сбор и разглашение посредством передачи) данных посетителей указанного сайта при размещении на сайте социального плагина Facebook в виде веб-кнопки «Нравится». При этом владелец сайта обязан информировать посетителей сайта об обработке

---

[126] The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid. Press release № 117/15, 6 October 2015. https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf

[127] Judgment of the Court, Case C230/14, 1 October 2014. http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30ddaeee4666aaf8474e8ec3817bab8f982e.e34KaxiLc3qMb40Rch0SaxuRb3j0?text=&docid=168944&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=305205

[128] Judgment on case C-210/16. Decision on 05/06/2018 http://curia.europa.eu/juris/liste.jsf?num=C-210/16

их персональных данных и получать согласия посетителей на нее (включая передачу данных в Facebook). Сам владелец сайта не несет ответственность за дальнейшую обработку полученных Facebook персональных данных посетителей. Несмотря на то, что в основе решения указаны положения не действующей Directive 95/46/EC, позиция Суда и описание ситуации само по себе остается актуальным[129].

К юрисдикции Европейского Суда по правам человека отнесено рассмотрение дел о нарушениях Европейской конвенции о защите прав человека и основных свобод. В деле Роман Захаров v. Российская Федерация, заявитель утверждал о тайном прослушивании его телефонных переговоров в России и об обязанности мобильных операторов установить оборудование, позволяющее правоохранительным органам проводить оперативно-розыскные мероприятия без достаточного законного основания, что составляло дозволенное скрытое прослушивание переговоров. Суд признал, что подобные действия нарушают статью 8 Европейской конвенции (право на уважение частной и семейной жизни), указывая, что положения российского законодательства, регулирующие прослушивание переговоров, не обеспечивают достаточных гарантий защиты от произвола и риска злоупотреблений, свойственных любой системе тайного наблюдения, и которые особенно высоки в таких странах как Россия, где службы безопасности и полиция имеют непосредственный доступ к данным мобильной коммуникации. В судебном решении указываются недостатки российского законодательства, одним из которых является доступность средств защиты только для лиц, которые имеют доказательства прослушивания, а получение такого доказательства невозможно в отсутствие системы оповещений и возможности доступа к информации о прослушивании[130]. Рассматривая дело Ben Faiza v. France Суд также пришел к выводу, что определение геолокации в реальном времени с помощью GPS в 2010 году в условиях отсутствия достаточного законодательного регулирования степени и пределов дискреционных полномочий властей, является нарушением права на уважение частной и семейной жизни. В особенности, принимая во внимание, что заявитель не мог воспользоваться минимальной защитой, предоставляемой законом в демократическом обществе[131].

В деле Shimovolos v. Russia Суд рассматривал обстоятельства регистрации правозащитника в «базе данных слежения», которая включала информацию о его передвижениях на поезде и самолете в пределах России и об аресте. База была создана на основании распоряжения министерства, которое не публиковалось. В итоге, Суд установил, что российское законодательство не

---

[129] Judgment on case C-40/17. Decision on 29/07/2019 http://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&doclang=EN

[130] Постановлении ЕСПЧ от 04.12.2015 по делу “Роман Захаров против Российской Федерации (Roman Zakharov v. Russia)” (жалоба № 47143/06) http://europeancourt.ru/tag/roman-zaxarov-protiv-rossii/

[131] Ben Faiza v. France. 8 February 2018. http://hudoc.echr.coe.int/eng-press?i=003-5999245-7685292

содержит достаточно четких пределов и способов реализации предоставленных властям дискреционных полномочий собирать и хранить информацию о частной жизни лиц в базе данных, а также не устанавливает доступных для общественности способов защиты от злоупотреблений. Проведенное исследование и выводы свидетельствуют о нарушении права на уважение частной и семейной жизни и права на свободу и личную неприкосновенность (статьи 8 и 5 Европейской конвенции соответственно)[132]. Похожие выводы излагает Суд при рассмотрении дела Szabó and Vissy v. Hungary об узаконенном законодательством Венгрии скрытом антитеррористическом наблюдении. На основании приведенных примеров судебных дел можно прийти к выводу, что нарушение права на уважение частной и семейной жизни возникает в случае распространения мер слежения на любое лицо, независимо от первоначально установленных пределов, отсутствия оценки действительной необходимости таких мер и возможности получения компенсации[133].

В отношении систем слежения Суд указывает на риски их использования, поскольку слежение в целях защиты национальной безопасности может подорвать или даже разрушить демократическое общество. В этой связи важно наличие адекватных и действенных правозащитных гарантий от злоупотреблений, также необходимо учитывать обстоятельства природы, охвата и продолжительности возможных мер слежения, оснований их применения, какие органы уполномочены разрешать, применять и контролировать такие меры, средства защиты, предусмотренные национальным законодательством[134].

В деле Aycaguer v. France Суд встает на сторону заявителя, признавая, что привлечение к уголовной ответственности за отказ выполнить требование предоставить биологический образец для включения в национальную базу данных, является нарушением права на уважение частной и семейной жизни. Суд мотивировал решение тем, что положения законодательства о хранении информации в базе данных не обеспечивают достаточной защиты субъектов, предоставивших данные, поскольку не содержат условий о дифференциации периодов хранения данных и о возможности их удаления. В результате законодательство не обеспечивает надлежащего баланса публичных и частных интересов[135]. В случае невозможности удалить персональную информацию из базы данных полиции, несмотря на прекращение производства в отношении заявителя, Суд также приходит к выводу о нарушении статьи 8 Европейской

---

[132] Shimovolos v. Russia. 21 June 2011. http://hudoc.echr.coe.int/eng-press?i=003-3581541-4053078

[133] Szabó and Vissy v. Hungary. 12 January 2016. http://hudoc.echr.coe.int/eng-press?i=003-5268616-6546444

[134] Klass and Others v. Germany, 6 September 1978, Kennedy v. the United Kingdom, 18 May 2010; Shimovolos v. Russia, 21 June 2011 https://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf

[135] Aycaguer v. France. 22 June 2017. http://hudoc.echr.coe.int/eng?i=001-174441

конвенции. Довод о хранении информации на протяжении 20 лет признан Судом как по сути неопределенный период времени[136].

В целом, статья 8 Европейской конвенции имеет целью защиту личной информации, которая не предполагается к опубликованию без согласия субъекта, такой как домашний адрес, частная и семейная жизнь подразумевает личный характер коммуникации, которая включает защиту и конфиденциальность электронной почты, номера телефона, электронной переписки и других форм коммуникации[137]. Концепция частной жизни включает, в том числе, элементы, относящиеся к праву личности на изображение, то есть фотографии и видео, которые содержат изображение также подлежат защите по статье 8 Конвенции. Фактически, право на защиту изображения предполагает право личности на контроль использования его изображения, включая право отказаться от его публикации. Данное утверждение также распространяется на хранение изображений в общих и социальных сетях, поскольку они могут содержать чрезвычайно личную или даже приватную информацию о субъекте или его семье[138].

Как установил Суд в деле Youth Initiative For Human Rights v. Serbia некоммерческая организация имеет право запрашивать у спецслужб информацию о количестве людей, ставших субъектами электронного наблюдения, в рамках выполнения своей роли «общественного стража» ("public watchdog"). Отказ в предоставлении данной информации будет составлять нарушение права свободно получать и распространять информацию (статья 10 Европейской конвенции)[139].

В случаях публикации высказываний онлайн в отношении публичных должностных лиц, Европейский суд нередко становится на сторону заявителя. В деле Renaud v. France Суд пришел к выводу, что привлечение заявителя к уголовной ответственности за клевету и оскорбление мэра на сайте в сети интернет является несоразмерным законной цели защиты прав и репутации других лиц[140]. Границы дозволенной в отношении правительства или публичного лица критики должны быть шире, чем в отношении физического лица, поскольку

---

[136] Khelili v. Switzerland, no. 16188/07, 18 October 2011 https://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf

[137] Flinkkilä and Others v. Finland, no. 25576/04, 6 April 2010; Saaristo and Others v. Finland, no. 184/06, 12 October 2010, Alkaya v. Turkey, no. 42811/06, 9 October 2012 https://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf

[138] Sciacca v. Italy, no. 50774/99, Von Hannover v. Germany (no. 2) [GC], nos. 40660/08 and 60641/08, Verlagsgruppe News GmbH and Bobi v. Austria case, no. 59631/09, 4 December 2012 https://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf

[139] Youth Initiative For Human Rights v. Serbia 25 June 2013. https://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22003-4412824-5302120%22]}

[140] CEDH, AFFAIRE RENAUD c. FRANCE, 25 février 2010, 13290/07 https://www.doctrine.fr/d/CEDH/HFJUD/CHAMBER/2010/CEDH001-97515

в демократическом обществе действия и проступки правительства находятся под наблюдением «недремлющего ока» прессы и общественного мнения[141].

Блокировка доступа к сети интернет в отдельных случаях рассматривается как нарушение статьи 10 Европейской конвенции (право на свободу выражения мнения). Так, в деле Ahmet Yıldırım v. Turkey национальные суды вынесли решение о блокировке доступа к сайтам Google из-за предоставления услуги хостинга интернет-сайту, владелец которого был участником уголовного расследования, возбужденного из-за оскорбления памяти деятеля Mustafa Kemal Atatürk. В результате, заявитель в жалобе в Европейский Суд указал на невозможность доступа к своему собственному сайту из-за вынесенного решения, хотя ни он сам, ни его сайт никакого отношения к уголовному расследованию не имели, а вынесенная национальными судами мера нарушает его право свободно получать и делиться информацией и идеями. Суд признал нарушение прав заявителя и указал на произвольность мер и необоснованность блокировки доступа[142].

Аналогично в деле Cengiz and Others v. Turkey о блокировке доступа к ресурсу YouTube, который позволяет пользователям посылать, просматривать и делиться видео, Суд признал нарушение прав заявителей свободно получать и делиться информацией, указав, что, как и заявители, преподаватели университетов были лишены возможности доступа к ресурсу продолжительный период времени, и также могут обоснованно утверждать о нарушении своих прав. При этом, как было установлено в ходе разбирательства, турецкое законодательство не содержит положения, позволяющего национальным судам вынести решение о всеобщей блокировке доступа к сети интернет, в данном деле к ресурсу YouTube, из-за содержания одного из его материалов[143]. В решении по делу Kalda v. Estonia Суд пришел к выводу, что государство не обязано предоставлять осужденным доступ к сети интернет, однако в случае, если такой доступ все-таки предоставлен, ограничение доступа к определённым веб-сайтам должно быть достаточно обосновано, иначе такое ограничение составит ущемление права на получение информации[144]. Рассматривая доводы заявителей и признавая нарушение статьи 10 Европейской конвенции в деле Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary Суд отметил, что национальные суды Венгрии не учли необходимость баланса противоположных

---

141 Mosley v. the United Kingdom, 10 May 2011. https://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf

142 Case of Ahmet Yıldırım v. Turkey. 18 December 2012 https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-115705%22]}

143Cengiz and Others v. Turkey. 1 December 2015 https://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22003-5241080-6502267%22]}

144 Kalda v. Estonia 19 January 2016 https://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22003-5274809-6556598%22]}

прав, а именно, права на свободу выражения мнения и права на уважение деловой репутации[145].

Наибольший интерес для формирования дальнейшей судебной практики в России и Совете Европы представляют вынесенные 23 июня 2020 Европейским судом по правам человека 4 решения по 6 веб-сайтам, которые подвергались блокировкам на территории Российской Федерации. Решения касаются разных аспектов и разных норм российского блокировочного законодательства, которое применяется Роскомнадзором, однако всех случаях суд установил нарушение права заявителей на свободу выражения мнения (ст.10 Конвенции) и права на эффективное средство правовой защиты (ст.13 Конвенции) и присудил каждому из заявителей по 10 000 Евро в качестве компенсации.

По делу Харитонов[146] против России, который жаловался на то, что его сайт был заблокирован заодно лишь на основании того, что находится на том же IP-адресе, что и ресурс с противоправной информации, суд единогласно постановил, что блокировка по IP-адресу является крайней и несоразмерной мерой. В этом решении говорится, что не только действия, связанные с неизбирательной блокировкой веб-сайтов, нарушают Европейскую конвенцию о правах человека, но также и то, что национальные законы, используемые для оправдания таких блокировок, не содержат необходимых гарантий, что несовместимо с принципом верховенства права.

По делу Энгельс[147] против России общественная организация "Роскомсвобода" жаловалась на признание незаконным решения Анапского суда, которым была запрещена одна из веб-страниц Роскомсвободы, на которой размещались информация о различных технических средствах обхода блокировок. По мнению местной прокуратуры и суда с помощью этой информации пользователи могут получить доступ к «Книги Единобожия» Мухаммада ибл Суллеймана и прочим материалам из экстремистского списка Минюста. По этому делу ЕСПЧ установил, что из-за размытости законодательства российские власти могут заблокировать любой контент и сравнил удаление сведений о технологиях доступа к информации из-за риска их использования для поиска экстремистских материалов с попытками ограничить доступ к принтеру со ссылкой на то, что экстремистские материалы можно на нем распечатать.

---

[145] Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary. 2 February 2016. http://hudoc.echr.coe.int/eng-press?i=003-5288151-6577157

[146] Kharitonov v. Russia 23 June 2020 http://hudoc.echr.coe.int/eng?i=001-203177

[147] Engels v Russia 23 June 2020 http://hudoc.echr.coe.int/eng?i=001-203180

По делу Флавус и др. против России жалобы были направлены ведущими оппозиционными российским СМИ - grani.ru (ООО "Флавус"), ej.ru / Ежедневный журнал (ООО "Медиафокус") и kasparov.ru (Гарри Каспаров), которые с 2014 года блокируются по информации надзорного ведомства за распространение призывов к несанкционированным массовым мероприятиям и тенденциозное освещение "болотного дела". Во всех случаях ЕСПЧ установил отсутствие в российском законодательстве гарантий от чрезмерных и произвольных последствий от блокировок. Суд пришел к выводу, что российский закон не предоставляет владельцам веб-сайтов каких-либо процессуальных гарантий, способных защитить их от произвольного вмешательства. В случае вынесения судебных решений, владельцы веб-сайтов, несмотря на доступную информацию, не были извещены и привлечены к участию в процессе, а также были лишены возможности судебного пересмотра решений. Во всех случаях суд также установил несоблюдение принципов необходимости и пропорциональности, избыточный характер блокировки и отсутствие в российском законе прозрачных процедур информирования владельца веб-сайтов о причинах нарушений и обжалования таких решений. В своих решениях суд ссылается на Декларацию о свободе общения в Интернете, принятую Комитетом министров Совета Европы 28 мая 2003 года, Совместную декларацию о свободе выражения мнений и интернете от 1 июня 2011 года, доклад Специального докладчика ООН 2011 года по вопросу о поощрении и защите права на свободу мнений и их свободное выражение (A / HRC / 17/27), Замечания общего порядка № 34 по статье 19 Международного пакта о гражданских и политических правах, принятого на 102-й сессии 2011 года), а также тематический документ, опубликованный Комиссаром Совета Европы по правам человека в 2014 году и Рекомендации Комитета министров государствам-членам о свободе интернета, принятая Комитетом министров Совета Европы 13 апреля 2016 года.

Все эти нормы посвящены необходимости и пропорциональности блокировок информации в сети интернет и определяют общие принципы при принятии решений о фильтрации и блокировки контента. Значение вынесенных решений ЕСПЧ вряд ли можно переоценить для формирования дальнейшей правоприменительной практики в России, учитывая, что количество органов, имеющих право принимать решения о внесудебной блокировке, а также оснований для блокировки контента, сайтов и мобильных приложений увеличивается ежегодно. Стоит напомнить, что сразу после вынесения 4 решений о блокировке веб-сайтов, ЕСПЧ также приступил к коммуникации дел по Telegram.

Есть все основания полагать, что эти решения будут также не в пользу Российской Федерации, даже несмотря на то, что Роскомнадзор спустя 2 года вынес мессенджер из Единого реестра после длительных неудачных попыток его заблокировать. В жалобах по Telegram заявители также жаловались на нарушение ст. 8 Конвенции в связи с нарушением права на тайну частной жизни в связи с требованиями к Telegram о предоставлении информации, необходимой для декодирования сообщений, и принятии меры по ослаблению шифрования.

Национальные суды в том числе рассматривают большое количество дел, связанных с сохранением конфиденциальности, неприкосновенностью частной жизни, правомерностью сбора персональных данных, в том числе биометрических. Одним из известных дел является коллективный иск к компании Facebook по поводу распознавания лиц на фотографиях, которые пользователи загружают на сайт. В качестве основания иска указано нарушение закона о конфиденциальности биометрической информации штата Иллинойс. По закону компании обязаны получить письменное разрешение гражданина, прежде чем собирать отпечатки пальцев, сканировать лицо или собирать другие идентифицирующие биологические характеристики. Резиденты вправе предъявлять иски компаниям на сумму до 5000 долларов за каждое нарушение, что может привести к миллиардам долларов выплат при проигрыше коллективных исков. В итоге, представители Facebook согласились на выплату компенсации и компенсацию судебных издержек, что практически означает признание исковых требований[148]. В другом деле окружной суд Сиэтла в штате Вашингтон указал, что содержимое экрана блокировки телефона может быть использовано ФБР в суде в качестве доказательства по делу только в случае наличия ордера на разблокировку. В случае ареста у подозреваемого может быть изъят телефон, но следователи ФБР не могут использовать фотографию экрана блокировки, так как это нарушает право на неприкосновенность частной жизни[149].

[148] «Facebook заплатит $550 млн за распознавание лиц на фотографиях без разрешения пользователей» https://habr.com/ru/news/t/486254/

[149] United States District Court. Western District of Washington at Seattle. Case No. CR19-0115-JCC. https://cdn.arstechnica.net/wp-content/uploads/2020/05/gov.uscourts.wawd_.274574.73.0.pdf

РЕЗЮМЕ

Несмотря на относительно недавнее появление «цифровых» прав, регламентирующие их международные источники права, национальные нормы и правоприменительная практика межгосударственных судебных органов развиваются поступательным образом. Правовое регулирование функционирования сети интернет и отношений, складывающихся в связи с «цифровизацией» общества, постоянно совершенствуется, предоставляя субъектам большую защиту их прав и свобод и возлагая на государства соответствующие обязательства.

Международные нормы «мягкого» права имеют целью защитить наиболее уязвимых субъектов «цифровых» отношений, наделяют их правами и рекомендуют идеальную модель возможной реализации предоставленных прав и свобод. Разрабатывая и принимая политики и законы в сфере использования сети интернет, государства, с одной стороны, стремятся соблюсти интересы личности, выполнить возложенные на них международные обязательства, но с другой, узаконивают механизмы ограничения «цифровых» прав, осуществления выгодных бизнес-моделей, предоставления дискреционных полномочий органам в области слежения и ограничения доступа к интернет-ресурсам, что на практике приводит к противоречиям и спорам, часто передаваемым на рассмотрение судов. Исчерпав внутригосударственные средства защиты, заявители обращаются в международные судебные органы, которые позволяют прийти к компромиссу между защитой предоставленных заявителям прав и соблюдением других установленных прав и требований. И несмотря на отступление некоторых стран, таких как РФ и КНР, от рекомендательных стандартов ООН и органов Совета Европы в части обеспечения цифровых прав, необходимо отметить значительный прогресс некоторых национальных законов в вопросе закрепления «цифровых» прав граждан. Во многих государствах признаны основополагающие права на доступ к сети интернет, свободу выражения мнений и коммуникации on-line, защиту информации и персональных данных. Несмотря на существующие неопределенности в использовании государствами технологий слежения, намечается тенденция совершенствования законодательства в данной области через установление оснований, пределов, сроков, технологий слежения и открытости сведений о лицах, в отношении которых используются меры слежения. В отдельных государствах создаются организации с общественным участием, которые уполномочены контролировать соблюдение законодательства в интернет-сфере.

РЕКОМЕНДАЦИИ ПО ПРИВЕДЕНИЮ В СООТВЕТСТВИЕ НАЦИОНАЛЬНОГО ЗАКОНОДАТЕЛЬСТВА

Отмечая необходимость правового обеспечения цифровых прав граждан при реализации национальной программы "Цифровая экономика", в целях приведения норм действующего законодательства в соответствие с положениями международного права и общепринятыми стандартами регулирования отношений, складывающимися в киберпространстве, а также устранения имеющихся правовых коллизий, рекомендуем Правительству Российской Федерации, Законодательному собранию Российской Федерации, АНО "Цифровая экономика" и всем другим заинтересованным сторонам принять во внимание следующие рекомендации:

1. Привести в исполнение решения ЕСПЧ по делу Zakharov v. Russia, Shimovolos v. Russia по созданию эффективных правовых средств контроля за обеспечением тайны связи и тайны частной жизни, в том числе:

   1.1. Разработать и внедрить систему оповещения граждан о состоявшемся перехвате трафика, сообщений, получении геолокационных данных, обработки биометрических данных человека, когда такие меры отменены либо достигнута законная цель.

   1.2. Создать независимый надзорный орган с общественным контролем по обеспечению приватности, который получит текущие полномочия Роскомнадзора по защите персональных данных, а также полномочия по осуществлению дознания в части совершения преступлений (в том числе должностных), посягающих на тайну частной жизни.

2. Привести в исполнение решение ЕСПЧ по делу Kablis v. Russia по созданию прозрачных и соразмерных механизмов ограничения доступа к противоправной информации, в том числе:

   2.1. Пересмотреть ст. 15.3 Федерального закона №149-ФЗ "Об информации" в части предоставления Генпрокуратуре слишком широкого усмотрения как в отношении оснований для блокировки, так и в отношении ее масштаба.

   2.2. Отказаться от практики внесудебного ограничения доступа к информации в сети интернет в пользу существующих механизмов принятия обеспечительных мер в судебном порядке по заявлениям органов прокуратуры, а также пересмотреть соответствующие нормы ст. 15.1-15.9 Федерального закона №149-ФЗ "Об информации"

3. Исключить из статьи 15.1 Федерального закона 149-ФЗ “Об информации” подпункт 2 пункта 2, что в реестр включаются: «2) сетевые адреса, позволяющие идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено», так как включение в Единый реестр дефицитных IPv4 адресов ведет к невозможности их использования и ограничению доступа к множеству иных ресурсов, находящихся на тех же IP-адресах.

4. Отменить Федеральный закон от 29.07.2017 №241-ФЗ "О внесении изменений в статьи 10.1 и 15.4 Федерального закона "Об информации, информационных технологиях и о защите информации", обязывающий интернет-мессенджеры идентифицировать пользователей по номеру мобильного телефона, как нарушающий право пользователей на анонимность и свободу информации.

5. Отменить Федеральный закон от 29.07.2017 №276-ФЗ "О внесении изменений в статьи 10.1 и 15.4 Федерального закона "Об информации, информационных технологиях и о защите информации", ограничивающий работу VPN-сервисов, Tor, анонимайзеров и нарушающий право пользователей на использование инструментов анонимизации и шифрования, свободу информации.

6. Пересмотреть положения Федерального закона от 06.07.2016 № 374-ФЗ

6.1. отменить п.3 ст. 10.1 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (“закон Яровой”) в части возложения обязанности на организаторов распространения информации в сети интернет хранить на территории РФ текстовые сообщения пользователей сети «Интернет», голосовую информацию, изображения, звуки, видео-, иные электронные сообщения пользователей сети «Интернет» до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки.

6.2. отменить п.4.1 ст.10.1 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (“закон Яровой”) в части возложения на организаторов распространения информации обязанности представлять в ФСБ России необходимую для декодирования принимаемых, передаваемых, доставляемых и (или) обрабатываемых электронных сообщений.

7. Обеспечить реализацию гражданами права получать информацию о том, какие государственные органы и частные компании получали доступ к их персональным данным, хранящимся в государственных информационных системах.

8. Установить законодательные гарантии режима “тихой гавани”, при котором информационные посредники не несут гражданской и

административной ответственности за размещаемый пользователями контент, в случае если размещение и распространение такого контента запрещено нормами действующего законодательства (по аналогии со ст.1253.1 ГК РФ).

9. В целях устранения правовой неопределенности внести изменения в ст. 10.3 Федерального закона № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (“право на забвение”), учитывая следующее:

9.1. Определить понятие “актуальности” информации, являющегося чрезмерно широким критерием для оценки того, должна ли информация оставаться доступной для широкой аудитории.

9.2. Сформулировать исключения для личной информации, имеющей общественную значимость и (или) касающейся общественных и политических деятелей.

9.3. Определить, какие действия должен принять поисковый сервис, так как из текущей нормы не ясно обязана ли поисковая система удалять оспариваемые ссылки в целом, либо она обязана удалять результаты поиска по имени определенного лица.

9.4. Установить гарантии от злоупотреблений путем обеспечения права владельцев веб-сайтов, к которым ведут оспариваемые ссылки, быть оповещенными о том что в отношении их содержания было подано требование в рамках «права на забвение», а также обязать операторов поисковых систем публиковать отчеты в рамках информационной открытости, содержащие достаточно подробную информацию о природе, объеме и результате рассмотрения требований, полученных в рамках «права на забвение».

10. Внести изменения в действующее антипиратское законодательство (ст. 15.2, ст.15.7 №149 “Об информации”), в том числе:

10.1. Ввести обязательный досудебный порядок урегулирования спора по делам, связанным с нарушением исключительных прав (аналог -DMCA);

10.2. Установить формальные процедуры для предоставления такого способа охраны исключительных прав как “блокировка сайта”. Для этого внести изменения в п. 4 ст.1259 ГК РФ указав статью в следующей редакции “для возникновения, осуществления и защиты авторских прав не требуется регистрация произведения или соблюдение каких-либо иных формальностей, кроме случаев, прямо предусмотренных действующим законодательством”, а также внести изменения в ст.15.2.,15.6 №149-ФЗ “Об информации”, указав что действие статьи и соответствующего способа защиты как ограничение доступа к сайту распространяется только на произведения, идентифицированные и зарегистрированные в установленном Правительством РФ порядке. Порядок

регистрации произведений (на основе НРИС либо DOI) разработать и утвердить Постановлением Правительства РФ;

10.3. Установить в качестве суда кассационной инстанции Суд по интеллектуальным правам для пересмотра в порядке кассации решений Мосгорсуда об ограничении доступа к веб-сайтам;

10.4. Отменить норму, введенную Федеральным законом №364-ФЗ и соответствующую ей ст.15.6 («Порядок ограничения доступа к сайтам в сети Интернет, на которых неоднократно и неправомерно размещалась информация, содержащая объекты авторских и (или) смежных прав, или информация, необходимая для их получения с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет»), о недопустимости снятия ограничений доступа к интернет-ресурсам даже в случае удаления контента, по которому состоялось решение о запрещении его распространения.

11. Обеспечить прозрачность и подотчетность органов государственной власти по ограничению доступа к противоправной информации, в том числе:

11.1. Возложить обязанность на государственные ведомства публиковать с периодичностью один раз в полгода отчеты о их деятельности в рамках правоприменения законодательства, регулирующего распространение информации в сетевом пространстве. Отчет должен содержать детальную статистическую информацию, а также аналитические материалы, которые показывают корреляцию деятельности госорганов по ограничению доступа к той или иной категории информации с положительной (или отрицательной) динамикой решения тех проблем, целью которых стоит запрещение распространение информации.

11.2. Реализовать создание общедоступного электронного каталога в машиночитаемом виде по всем вынесенным решениям со стороны государственных органов и судов по признанию той или иной информации (и тех или иных интернет-ресурсов) запрещенной к распространению в России в рамках реализации государственной инициативы по предоставлению гражданам РФ открытых данных о деятельности органов законодательной/исполнительной власти и судов.

12. Ввести законодательный мораторий на использование "технологии распознавания лиц" правоохранительными органами и органами надзора, а также приостановить работу по нормативно-правовым актам о цифровом профиле[150], цифровых паспортах[151] и информационном регистре[152] до принятия правовых гарантий от злоупотреблений и утечек данных, а также механизмов

[150] https://roskomsvoboda.org/47060/

[151] https://regulation.gov.ru/p/102582

[152] https://sozd.duma.gov.ru/bill/759897-7

надлежащего надзора. Мораторий должен применяться к любому виду разработки нормативных актов, создания и поддержания федеральных и региональных программ, предоставления федеральных субсидий и помощи субъектам РФ, которые стремятся использовать технологии распознавания биометрических данных человека в правоохранительных целях либо для контроля за передвижением граждан.