МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ ГОСУДАРСТВА И ПРАВА
Кафедра теоретических и публично-правовых дисциплин

РЕКОМЕНДОВАНО К ЗАЩИТЕ В ГЭК
И.о. заведующего кафедрой
канд.юрид.наук, профессор
О.Ю. Винниченко
«___» _____2021

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
магистерская диссертация

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ: ВНУТРИГОСУДАРСТВЕННАЯ И МЕЖДУНАРОДНО-ПРАВОВАЯ РЕГЛАМЕНТАЦИЯ

40.04.01 Юриспруденция (уровень магистратуры)
Магистерская программа «Защита прав человека и бизнеса»

Выполнил работу
Студент 3 курса
заочной формы обучения — Мовсисян Нарине Робертовна

Научный руководитель
канд. юрид. Наук,
доцент — Яковлев Александр Александрович

Рецензент
Адвокат — Грибанова Анастасия Александровна

Тюмень
2021

СОДЕРЖАНИЕ

СПИСОК СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

АТЭС - Азиатско-Тихоокеанское экономическое сотрудничество
ЕС – Европейский союз
ЗПД – Защита персональных данных
КНР – Китайская Народная Республика
МСЭ - Международный союз электросвязи
ОЭСР - Организация экономического сотрудничества и развития
ПДН – Персональные данные
РФ – Российская Федерация
СМИ – Средства массовой информации
США – Соединенные Штаты Америки
ТТП - Транстихоокеанское партнёрство
ФАС – Федеральная антимонопольная служба
ФЗ – Федеральный закон

ВВЕДЕНИЕ

Одной из отличительных тенденций в современном мире является то, что многие страны международного сообщества координируют свои усилия в попытке сформировать глобальное информационное сообщество. Информационным сообществом называют объединение, работа членов которого зависит от информационных потоков, имеющихся у них знаний и навыков, а также современных технологий. Взаимоотношения между членами информационного общества будут зависеть как раз от этих условий, а экономика в нем будет основана на продуктах интеллектуальной и информационной систем.

На начальном этапе информационным обществом может являться объединение стран по какому-либо признаку, как правило, уже достигших определенных параметров в области экономики и социологии. Но главным критерием при объединении таких страх будет уровень развития современных технологий и компьютеризации общества и его членов, науки, образования и культуры. Экономическое процветание таких стран, а также культурное развитие жителей страны зависит от степени развития указанных параметров. Очевидно, что принадлежность к такому обществу не исключает и национальных интересов государства, и необходимости защиты этих интересов. Именно поэтому при организации международного сообщества важно защищать национальные интересы в информационной сфере.

В Российской Федерации предпринимаются шаги по созданию суверенного Интернета как единой, унифицированной, централизованной информационно-телекоммуникационной сети, в отношении которой государство будет обладать функциями контроля и управления (сетями общего пользования)[1], проводя политику импортозамещения информационно-коммуникационных средств, устанавливая законодательное регулирование, выстраивая отношения в Интернете на основе приверженности национальным интересам в целях противодействия

[1] Постановление Правительства РФ от 13 февраля 2019 г. N 136 «О Центре мониторинга и управления сетью связи общего пользования» // СПС «Консультант Плюс»

потенциальным угрозам, а также способности проводить политику в условиях национальной юрисдикции.

В соответствии с недавним исследованием, проведенным международной компанией Positive Technologies, порядка 8-10% всех совершенных кибератак (в мире) приходится на Россию[1]. Указанная статистика свидетельствует о том, что Россия в настоящее время занимает второе место по числу совершенных кибератак. Тем не менее, статистические данные по исследуемому вопросу нередко расходятся. Так, согласно стат. данным Международного союза электросвязи, в настоящий момент Россия занимает 28 место в рейтинге стран по индексу кибербезопасности[2]. Так или иначе, означенные показатели свидетельствуют о необходимости совершенствования механизмов защиты конфиденциальных сведений в современных условиях всемирной компьютеризации и цифровизации. Заметим, что по данным 2021 года МСЭ Россия заняла 5-е место в рейтинге кибербезопасности ООН, получив 98 баллов из ста возможных. Это не может не радовать. Несмотря на связанные с COVID-19 проблемы, а именно переиначивание всех сфер жизни, социально-экономических услуг в цифровую сферу, Россия за последние два года смогла значительно повысить свой индекс кибербезопасности и показать отличный результат. В отличие от 2018 года, на данный момент ведется тенденция к принятию национальных стратегий по кибербезопасности, а так же повышение осведомленности в этой области в настоящее время. Нельзя не отметить, что новый темп дистанционной жизни в связи с COVID-19 оставил след и на вовлечении стран в реализацию кибербезопасности своего государства. Россия не исключение.

Базовым понятием в рамках исследования является «защита персональных данных». Федеральный Закон №152 «О персональных данных» дает

---

[1]Ли И. Россия стала второй после США по количеству кибератак [Электронный ресурс] // РБК. URL: https://www.rbc.ru/technology_and_media/13/06/2017/593a9a749a794766d6b11c54 (дата обращения: 16.10.2021).

[2] Global Cybersecurity Index [Электронный ресурс] // Committed to connecting the world. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf (дата обращения: 16.10.2021).

исчерпывающее определение данного понятия. Оно содержит следующую формулировку: «персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)»[1]

Объектом настоящего исследования выступает элемент государственного суверенитета, проявляющегося в сфере информационных технологий. Предметом исследования является институт защиты персональных данных в информационно-телекоммуникационной сети интернет.

Цель работы: провести анализ внутригосударственных и международно-правовых регламентаций в сфере защиты персональных данных.

Для достижения вышеуказанной цели видится важным обозначить задачи настоящей работы: проанализировать основные положения отечественного законодательства в сфере обеспечения информационной безопасности, изучить статистические показатели означенной сфере; ознакомиться с материалами судебной и иной правоприменительной практики, выявить пробельные положения законодательства о защите персональных данных; обозначить перспективы государственного регулирования в сфере информационной безопасности; проанализировать опыт зарубежных правопорядков по обеспечению защиты конфиденциальных сведений в информационной сфере, а также провести сравнительно-правовой анализ документов стратегического планирования;

В первой главе работы рассматриваются теоретические положения, связанные с вариативностью определения базовых понятий, а также рассматривается судебная практика Российской Федерации по защите персональных данных субъектов. Во второй главе анализируются направления государственной политики КНР по регулированию защиты персональных данных, а так же рассматривается применимое право к транснациональным персональным данным человека в контексте вируса COVID-19. Третья глава отражает

[1] Собрание законодательства Российской Федерации. 2006. № 31 (1 ч.) Ст. 3451.

международно-правовые акты, международные договоры по защите персональных данных.

Новизна настоящей работы состоит в определении характеристических черт особенностей государственной политики в сфере нормативно-правового регулирования защиты персональных данных, их отличий от зарубежного опыта. Новизна данной работы также определяется рядом предложений по совершенствованию отечественного законодательства в сфере защиты конфиденциальной информации.

Глава 1. ВНУТРИГОСУДАРСТВЕННОЕ РЕГУЛИРОВАНИЕ: РОССИЙСКАЯ ФЕДЕРАЦИЯ

1.1. Правовое обеспечение информационной безопасности персональных данных в сети Интернет.

Возникновение ИПД (института персональных данных) в отечественной практике было связано, прежде всего, с принятием ФЗ «О персональных данных» и ряда других федеральных законов. В соответствии с указанным нормативным актом, занявшим ключевую роль в правовом регулировании защиты информации, персональными данными признаются данные о физических лицах, способных их идентифицировать, т. е. обнаружить, выделить среди прочих граждан. Важно отметить, что закон не устанавливает исчерпывающего перечня персональных данных, что следует признать вполне обоснованным. В самом деле, в условиях интенсивного развития информационных технологий, качественного влияния процессов информатизации и цифровизации[1] на многие общественные, в том числе правовые институты, стремительное появление новых данных, носящих конфиденциальный характер, стало вполне обычным явлением.

В связи с вариативностью и разнородностью персональных данных в доктрине и правоприменительной практике принято дифференцировать их различным классификационным основаниям. Так, используя такой критерий как характер персональных данных, их можно подразделить на общие персональные данные и так называемые деликатные персональные данные[2]. К общим персональным данным принято относить информацию, позволяющую установить определенное лицо (идентифицирующие характеристики субъекта персональных данных), как-то: место жительства, уровень дохода, полученное образование, номер телефона, иные контактные данные, регистрационные, паспортные данные. Отличие деликатных персональных данных от общих состоит в их зависимости от их носителя — субъекта персональных данных, и, следовательно, характера

---

[1] Михасева Е. А. Транспарентность правосудия и защита персональных данных // Теоретико-прикладные проблемы реализации и защиты субъективных прав в контексте инновационного социально-экономического развития общества. 2018. С. 510.

[2] Пыск Д. А. Первый взгляд на закон о защите персональных данных // Проблемы науки. 2018. № 4 (28). С. 93.

подобной информации. К деликатным персональным данным можно отнести социальные, религиозные, политические, экономические, правовые и иные взгляды и позиции личности. Представляется, что все перечисленные виды конфиденциальной информации должны квалифицироваться как персональные данные и подлежать публично-правовой охране.

Ряд авторов положительно отмечает смысловое содержание ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации», закрепляющие руководящие положения об информации. Так, приведенной статьей сообщаются дефиниции таких понятий как информация, информационная система, информационные технологии, информационно-телекоммуникационная сеть, информационные технологии и т.д. Тем не менее, видится необходимым идти дальше означенных дефинитивных норм и выводить из ст. 2 виды информационных технологий и информации соответственно, в отношении которых должны приниматься меры по охране и защите конфиденциальных сведений. Так, принято различать следующие виды информационных технологий: высокие интеллектуальные информационные технологии, вспомогательные информационные технологии и коммуникативные информационные технологии.

Для выработки эффективных правовых механизмов защиты персональных данных законом сформулирован ряд определений. Так, в соответствии со ст. 3 Федерального закона «О персональных данных» оператором персональных данных признается государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия, совершаемые с персональными данными. Субъектом данных являются любые физические лица, персональные данные которых обрабатываются (или с которыми совершаются иные установленные законом операции). Обработкой персональных данных признается деятельность, связанная со сбором, записью, хранением, использованием, удалением конфиденциальной информации.

Основным недостатком нормативно-правового регулирования интситутов защиты персональных данных выступает недостаточная доработка законодательной базы. Более того, ввиду постоянных сложностей, связанных с развитием информационных технологий в условиях всеобщей компьютеризации и цифровизации, нормативно-правовые акты устаревают и требуют развития, воспроизводства и дополнений. Существующие на сегодняшний день способы блокировки доступа к различным интернет-сайтам и ресурсам обеспечивают защиту данных недостаточно хорошо, ведь по-прежнему существует огромное количество способов обхода существующих фильтров, которые совершенствуются и улучшаются день за днем, соответствуя развитию инструментов управления трафиком[1].

В отличие от привычных СМИ, средства информационно-телекоммуникационной сети «Интернет» на протяжении долгого времени оставались законодательно неурегулированными. Означенное обстоятельство было связано с незначительной долей проникновения Интернета в масштабах РФ, которая в 2008 году составляла около 12%, а через десять лет уже выросла до 64% населения страны[2].

Глобальная паутина стала оказывать значительное влияние на жителей страны, деятельность фирм, политические действия, государство в целом благодаря воздействию информационного таргетинга, непредсказуемых хакерских атак и иных механизмов воздействия.

---

[1] Балашов А.Н. Правовое регулирование Интернет - отношений: основные проблемы и практика реализации в России [Электронный ресурс] // Cyberleninka. URL: https://cyberleninka.ru/article/n/pravovoe-regulirovanie-internet-otnosheniy-osnovnye-problemy-i-praktika-realizatsii-v-rossii (дата обращения: 15.10.2021).

[2] Интернет в России: динамика проникновения. Зима 2017–2018 гг. [Электронный ресурс] // ФОМ. URL: https://fom.ru/SMI-i-internet/13999 (дата обращения: 15.09.2021)

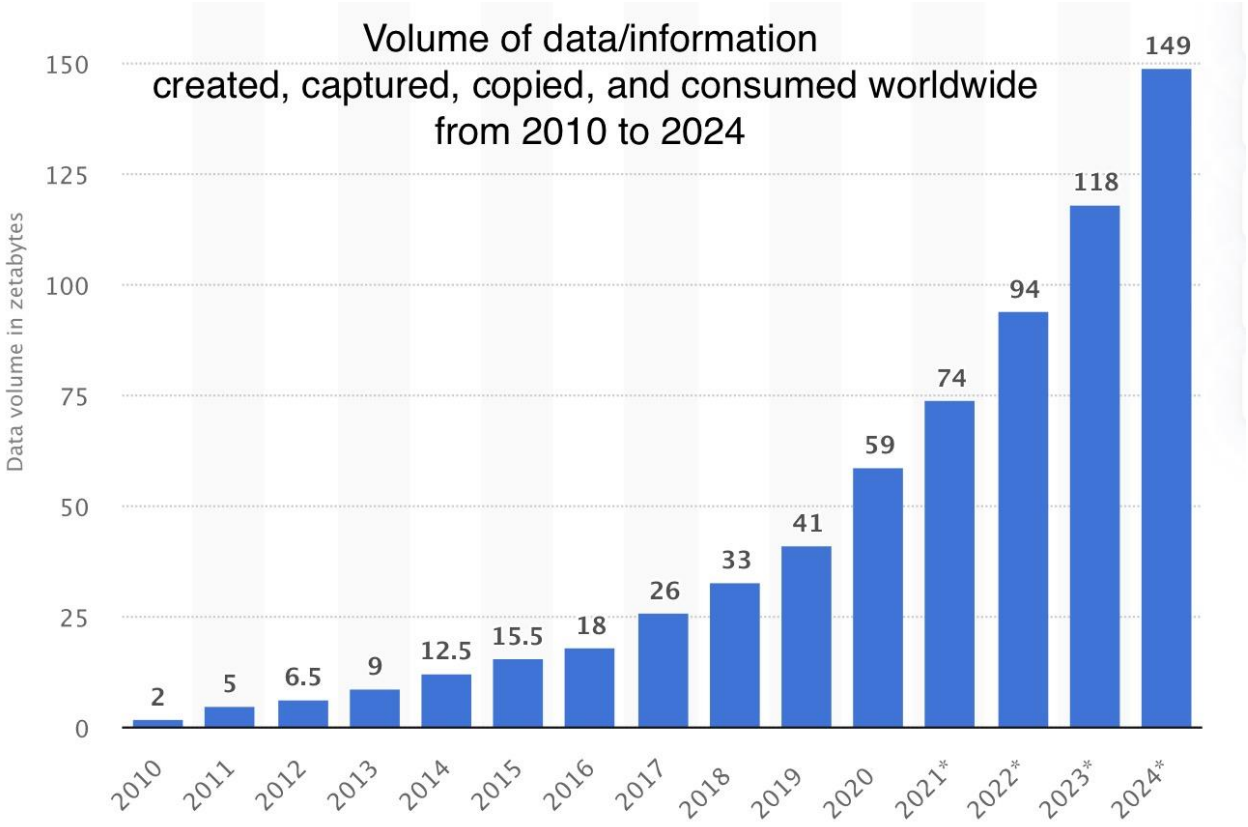

Рис. 3. Динамика проникновения Интернета в 2010-2021 гг. Прогноз до 2024 г.

Многие ученые в области изучения информационных технологий, считают, что Интернет должен регулироваться на надгосударственном уровне. Это может не только способствовать унификации отношений, необходимой для трансграничного характера глобальной сети, но и стать сложно реализуемым процессом[1]. Ведь в России отсутствует унификация законодательства и механизмы регулирования сети Интернет не укомплектованы в единую систему, а обеспечение суверенитета информационной сферы в разных государствах сильно отличается.

Президентом России был подписан Федеральный закон от 1 мая 2019 г. № 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации» , который вступил в силу в 1 ноября 2019 г. В нем определяются необходимые правила маршрутизации сообщений электросвязи; создается возможность для минимизации передачи за рубеж данных, которыми обмениваются между собой

[1] Shaw S. R. There is no silver bullet: solutions to Internet jurisdiction // International Journal of Law and Information Technology. 2017. Т. 25. №. 4. С. 283-308.

российские пользователи; урегулированы отношения в передаче во владение трансграничных линий связи; операторы связи и управляющие точками обмена информационного трафика должны обеспечить безопасность глобальной сети Интернет при возникновении различных угроз, нарушений функционирования и различных атак. Трафик должен регулироваться централизованно, а безопасность будет обеспечиваться с помощью установки современных инструментов противодействия угрозам; создается инфраструктура, позволяющая обеспечить работоспособность российских интернет-ресурсов в случае невозможности подключения российских операторов связи к зарубежным корневым серверам сети «Интернет».

В рамках реализации закона планируется создание и использование российского программного обеспечения для обеспечения безопасности и защиты информационного пространства государства от воздействия любых внешних и внутренних угроз.

В настоящее время в Российской Федерации политика по регулированию и суверенизации Интернета по большей части осуществляется путем реализации Доктрины информационной безопасности, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. № 646[1] и вытекающих из нее показателей и мероприятий, содержащихся в государственной программе «Информационное общество», утвержденной постановлением Правительства Российской Федерации от 15 апреля 2014 г. № 313[2] , а также национальной программе «Цифровая экономика в Российской Федерации», утвержденной протоколом президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 24 декабря 2018 г. № 16[3]

Табл. 1

Особенности структуры и содержания Доктрины информационной

[1] Собрание законодательства Российской Федерации. 2016. № 50. Ст. 7074.
[2] Собрание законодательства Российской Федерации. 2014. № 18. Ст. 2159.
[3] Документ опубликован не был

безопасности РФ[1]

Структурный элемент	Описание
Основная цель	Защита интересов государства от внутренних и внешних воздействий, угрожающих безопасности и связанных с современными технологиями в области информации в политических целях, противоречащих международному праву
Прогнозируемые на долгий период цели и главные сферы, в которых необходимо обеспечение безопасности информации	Раздел раскрывается в следующих сферах информации: оборона, безопасность страны и ее жителей, экономика, наука, образовательная система, многолетняя стабильность, современные технологии и равноправное стратегическое партнерство
Организационные моменты обеспечения безопасности в области информации	Определены уполномоченные органы, участники, а также принципы: 1. Законность общественных отношений в информационной сфере и правовое равенство всех участников таких отношений, основанные на конституционном праве граждан свободно искать, получать, передавать, производить и распространять информацию любым законным способом. 2. Эффективная обоюдная работа государственных органов, фирм и жителей страны по принятию решений в области обеспечения информационной безопасности. 3.Соблюдение баланса между потребностью граждан в свободном обмене информацией и ограничениями, связанными с необходимостью обеспечения национальной безопасности, в том числе в информационной сфере. 4. Эффективное распределение и достаточное обеспечение ресурсами для реализации информационной безопасности и непрерывного мониторинга воздействующих шумов 5.Соблюдение общепризнанных принципов и норм международного права, международных договоров Российской Федерации, а также законодательства Российской Федерации.

Законодательное основа базируется на Конституции Российской Федерации, Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» (далее - Закон об информации), Федеральном законе от 07 июля 2003 г. № 126-ФЗ «О связи» (далее - Закон о связи), Федеральном закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры

[1] Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 // Собрание законодательства Российской Федерации. 2016. №50. Ст. 7074.

Российской Федерации» (далее - Закон о критической инфраструктуре) и поправках к ним.

История становления и развития категории информационной безопасности свидетельствует о ее имманентной связи с носителями информации. Укрепление и совершенствование последних объективно усложняет способы обеспечения защиты информации как ценного ресурса постиндустриального общества. Глобальные процессы информатизации и цифровизации качественно повлияли на процесс развития правовых институтов. Так, например, с принятием в 2006 г. ФЗ «Об информации, информационных технологиях и о защите информации». была закреплена дефиниция, формы информации, формы её защиты[1] и тд. Не так давно в ст. 128 ГК РФ были внесены дополнения в части расширения объектов гражданского права, не ограниченных в обороте. Перечень указанных объектов был дополнен цифровыми правами.

1.2. Судебная практика по вопросам защиты персональных данных субъекта.

Любые нарушения ФЗ о персональных данных, выданные предписания Роскомнадзора и протоколы о привлечении к административной ответственности вынуждают юридических лиц прибегать к судебной защите. Существующая судебная практика неоднородна, но достаточно интересна. Уже сейчас можно сказать, что у судебной системы в РФ есть некоторый порядок действий по принятию решений по закону о защите персональных данных. Споры в судах рассматриваются разные, но, как правило, все они связаны не с осознанными нарушениями ФЗ о персональных данных, а с его непониманием.

Ключевые институты защиты персональных данных уже успели стать предметом многочисленных оспариваний в актуальной практике

[1] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ // СПС «КонсультантПлюс»

правоприменения. Представляется, что знание судебной и иной правоприменительной практики позволит операторам персональных данных, а также иных субъектам персональных данных избежать нарушений закона в исследуемой сфере

Так, например, Конституционный суд Российской Федерации провел слушание по вопросу конституционности нормы закона, запрещающей операторам предоставлять обрабатываемые ими персональные данные третьим лицам[1]. Заявитель, обратившийся за информацией о своих коллегах и получивший отказ оператора предоставить персональные данные, обратился в Конституционный суд, посчитав, что такой отказ нарушает его право на судебную защиту, поскольку ч. 4 ст. 29 Конституции РФ предусмотрена возможность свободного поиска и получения информации любыми способами, не запрещенными федеральным законодательством. Суд дал отказ заявителю, сделав упор на то, что право человека на защиту информации о его личной жизни является безусловным. Более того, по мнению юрисдикционного органа, Основной закон содержит императивный запрет на получение и реализацию информации о частной жизни лица без его согласия. Последний тезис находит свое подтверждение в актуальном нормативно-правовом регулировании, которое в качестве основного правила делает упор на конфиденциальность личных данных гражданина, и, таким образом, действует тотальный запрет на раскрытие личных данных, тем или иным образом относящихся к гражданину, и полученных от него каким-либо лицом (в том числе оператором данным). Таким образом, конституционно-правовое ограничение на собирание и распространение информации субъектов персональных данных является правомерным, поскольку позволяет обеспечить конфиденциальность соответствующей информации.

[1] Определение Конституционного Суда РФ от 26.05.2016 N 1158-О «Об отказе в принятии к рассмотрению жалобы гражданки Сазоновой Елены Александровны на нарушение ее конституционных прав статьей 7 Федерального закона "О персональных данных» // СПС «Консультант Плюс»

Кроме того, за нарушение закона о персональных данных гражданин может привлекаться к гражданско-правовой ответственности за совершенные действия в виде возмещения морального вреда тому, чьи данные были раскрыты. Так, например, в одном из материалов дела суд счел нарушением закона размещение издательством в газете фотографии человека и сведений о нем без заранее полученного на то одобрения данного человека. Таким образом, его персональные данные были раскрыты, а суд взыскал с издательства моральный ущерб за публикацию персональных данных гражданина.

Для любой фирмы, действующей на территории Российской Федерации, во время поиска и найма новых сотрудников на работу и продающей товары через интернет-источники, актуальным остается вопрос об обязательном уведомлении Роскомнадзора о своей деятельности по обработке персональных данных потенциальных работников в следующих случаях:

– сбор первичной информации о потенциальных работниках – ФИО, уровень образования, возраст и т.п., полученные из резюме, размещенном на сайтах или отправленных лично работодателю – данная информация вносится в единую базу компании;

– компания используем программы, цель которых обрабатывать персональные данные потенциальных нанимателей;

– компания обрабатывает персональные данные с использованием любых других методов фиксации информации.

Четвертый арбитражный апелляционный суд постановил во всех перечисленных выше случаях не обязательным уведомление нанимателя о начале работ по обработке его персональных данных.

Каждый из нас практически ежедневно самостоятельно раскрывает свои персональные данные, регистрируясь на различных сайтах, проходя опросы, заполняя различные анкеты, приобретая товар в сети Интернет, оформляя абонементы в спортзал и скидочные карты. Чаще всего, при совершении данных действий требуется подтвердить согласия на обработку персональных

данных и большинство из нас, не читая, соглашаются. Некоторые организации забывают о данном пункте и не просят подтвердить согласием политику обработки персональных данных, игнорируя по какой-то причине требования ФЗ. На самом деле, данные, передаваемые оператору, хранятся тщательно и в большинство случаев надежно. Однако, бывают ситуации, вызывающие уйму вопросов. Как, например, предоставление паспорта в магазине при возврате товара. Является ли данное действие предоставлением персональных данных? Суд установил, что данная ситуация не является нарушением законодательства о персональных данных. Ситуация возникла по обращению покупателя в ФАС РФ, который посчитал, что внесение паспортных данных в заявление о возврате продукции в магазин является обработкой персональных данных, которая не осуществляется в соответствии с требованиями закона. Магазин был оштрафован. Суд не стал связывать эту ситуацию с незаконной обработкой данных и отменил штраф.

Не менее интересной является публикация чужих фотографий. Фото может являться объектом, распространяющим персональные биометрические сведения физических лиц. Так, было установлено, что при использовании фотографии физического лица для оформления любого вида пропуска (на работу в офис, в бассейн) необходимо получить согласие этого лица на обработку его персональных данных. С 2013 года такое положение дел рассматривалось Роскомнадзором как спорная ситуация, не обязательная к исполнению, соответственно организации воспринимали это исключительно как рекомендацию, а не обязаловку. Однако, после решение суда по одному из подобных дел в пользу физического лица, стало необходимым оформление согласия на обработку персональных данных во избежание неприятных ситуаций с законом.

В самом деле, конфиденциальные данные окружают нас везде и всюду. Разумеется, такая вариативность персональных данных, подлежащих защите и государственно-правовой охране, во много связана с многообразием форм-носителей конфиденциальной информации. Письменные документы,

электронные документы, аудиозаписи и видеозаписи, фонограммы, материалы киносъемки — всё это может квалифицироваться как носители конфиденциальной информации о частной жизни граждан и подлежать соответствующей государственно-правовой защите. Разумеется, означенные носители информации нашли свое закрепление в различных законодательных актах как материально-правового, так и процессуально-правового характера. Тем не менее, различие с вышеуказанными носителями следует проводить не по формальному критерию (внешнему источнику, форме выражения), а по признаку содержательности, характера такой информации, носящей личный, частно-правовой характер, смысл которой и состоит в ее конфиденциальности, осведомленности о ее наличии лишь отдельных лиц.

Тем не менее, проблемы возникают систематически и повсеместно, будь то образовательная система или медицина. Руководители некоторых подразделений не всегда берут с клиентов согласие на обработку персональных данных. Например, в Самаре при оказании медицинских услуг персональные данные пациентов вносились в амбулаторные карты без согласия граждан на обработку персональных данных. Мировой суд постановил привлечь директора медицинской организации к административной ответственности по ст. 13.1 КоАП РФ и оштрафовал на 500 рублей. Областной Самарский суд встал на сторону мирового. Теперь, данная организация при оказании медицинских услуг и при внесении данных пациентов в любые базы и карты требует согласие пациентов на обработку их данных. Даже при оформлении отчетности, в которой фигурируют данные клиентов.

В целом, по всей России нарушений подобного характера на сегодняшний день не так много, а нарушители отделываются небольшими наказаниями в виде штрафов и предупреждений.

Интенсивное развитие информационных технологий и последующее активное использование их в различных сферах «человеческого общежития», определили ключевые векторы развития российской правовой системы. Так,

категориальный аппарат, функции, порядок использования информационных технологий нашли свое закрепление в системе российского законодательства; в 2006 году был принят Федеральный закон «Об информации, информационных технологиях и о защите информации», заложивший своим содержанием нормативную основу информационных технологий; глобальные процессы информатизации и цифровизации, с которыми традиционно связывают внедрение информационных технологий в правовую действительность, привнесли соответствующие изменения в некоторые положения гражданского законодательства, в частности, в ст. 128 ГК РФ, придавшую цифровым правам юридическую природу объектов гражданских прав. Практические аспекты развития и применения информации и информационных технологий в различных областях юридической деятельности были утверждены в некоторых подзаконных актах.

Так, в 2006 г. было принято постановление Правительства Российской Федерации «О федеральной целевой программе «Развитие судебной системы России» на 2007-2011 гг.», содержанием которого определялась необходимость создания единой информационной системы по размещению судебных актов в информационно-телекоммуникационной сети «Интернет», банков данных судебных решений, а также реализация иных перспективных направлений. Таким образом, общемировые процессы информатизации и цифровизации определили новый путь развития российской правовой системы.

ГЛАВА 2. АНАЛИЗ ИНОСТРАННОГО ОПЫТА В РЕГУЛИРОВАНИИ ВОПРОСОВ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ.

2.1. Направление политики регулирования защиты персональных данных человека: государственно-правовой опыт КНР и Казахстана

До недавнего времени можно было смело утверждать о том, что в КНР не существует как такового режима защиты персональных данных как бы это удивительно бы не звучало. До 2020 года в Китае не было общего закона «О защите данных», но его следы можно было бы проследить во множестве отраслевых правовых документах. Можно было бы говорить о «кумулятивном эффекте», характеризующем китайский подход к защите информации о человеке. Решительная разница между системами информационной защиты ЕС и КНР заключается в их базовом подходе к обработке персональных данных. Даже если пренебречь параметром прав человека ради анализа, факт – какая бы защита данных ни существовала сегодня в Китае, она во всяком случае направлена исключительно на человека как потребителя.

Основная, лежащая в основе концепция заключается в том, что защита данных является « инструментально необходимой для развития электронной коммерции”[1]. Получатель защиты данных — это не физическое лицо или “субъект данных», как в ЕС, а потребитель. В этом контексте, например, тот факт, что “каждый уголок Пекина теперь виден на правительственной сети камер наблюдения” без каких-либо слов о защите данных празднуется как “триумф” китайской полицией»[2].

Соответственно, положения о защите данных не направлены на обеспечение самоопределения или даже контроля над личной информацией человека, а скорее направлены на укрепление общественного доверия и стимулирование продаж. Однако этот подход несовместим с

---

[1] See Ess C, *Lost in Translation? Intercultural Dialogues on Privacy and Information Ethics* (Introduction to the special issue on Privacy and Data Privacy Protection in Asia)’ (2020) Ethics and Information Technology 7, 1–6.

[2] BBC News, *China surveillance cameras 'a triumph', say police*, 5 October 2019.

законодательством ЕС (или, для тех же целей, любым другим) о защите данных и скорее относится к сфере потребительского права. Мы установили, что это относится к большинству китайских правовых документов, якобы формулирующих китайский режим защиты данных, которые анализируются ниже.

В том же контексте следует иметь в виду, что защита данных - это система, которая не может и не должна быть разбита на ее конституционные части, чтобы иметь возможность строить сравнение и находить общие основания. Система защиты данных, даже если отойти от строгой модели защиты данных ЕС, подтверждается общими идеями, содержащимися во всех соответствующих международных документах, действующих сегодня: Директива Европейского Парламента и Совета Европейского Союза 95/46/ЕС от 24 октября 1995 г. «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных», Конвенции Совета Европы о защите данных, в частности «Конвенция о защите физических лиц при автоматизированной обработке персональных данных» (Заключена в г. Страсбурге 28.01.1981), руководящих принципах ОЭСР и рамках конфиденциальности АТЭС. Все они включают в себя набор основных принципов обработки данных (принципы справедливой информации) и набор основных прав на защиту данных (информация, доступ и возражение). Невозможно разбить эту систему на составляющие, потому что одна не функционирует без других. Например, нельзя найти в одном правовом акте принцип безопасности или конфиденциальности личной информации и, при полном отсутствии какого-либо другого принципа или индивидуального права, установить существование режима защиты данных. Это было бы вынужденным и контрпродуктивным упражнением. Абсолютный международный минимум защиты данных должен восприниматься как единое целое: принципы справедливой информации и основные права личности (европейцы также добавили бы к этому списку независимый механизм мониторинга). Если один из них отсутствует, то никакого режима защиты

данных не существует. Именно с этой точки зрения представляется возможные определение того, что Китай не имеет режима защиты данных. Вместо этого у него есть следы защиты данных, которые можно найти исключительно в его частном секторе обработки персональных данных.

В то время как вышеизложенное относится, в частности, к защите данных, защита частной жизни может быть гораздо лучше в соответствии с действующим китайским законодательством. Как будет показано ниже, право на неприкосновенность частной жизни, где, однако, “неприкосновенность частной жизни” воспринимается в Китае иначе, чем в Европе[1], закреплено в основном китайском законодательстве и действительно на самом высоком уровне, в конечном счете связано с правом на достоинство.

Наличие защиты частной жизни в Китае также облегчается тем фактом, что, в отличие от права на защиту данных, нет необходимости сопровождать его правовой системой, которая осуществляет его на практике, но его возникновение скорее устанавливается без посторонней помощи, на специальной основе. В любом случае, несмотря на то, что важные ограничения, очевидно, применимы и в этом случае, поскольку в соответствии с китайским законодательством государственный сектор и национальные цели, динамично определенные правящей Коммунистической партией, находятся вне досягаемости любого закона, китайским гражданам была предоставлена защита судами на основании нарушения их права на неприкосновенность частной жизни. С этой точки зрения, если бы защите данных было придано равное значение, как защите частной жизни, то “кумулятивный эффект”, рассмотренный выше, был бы существенно усилен. Однако это не так, по крайней мере в ЕС, где и договоры, и обширное прецедентное право четко различают их. Тем не менее, для целей настоящего

---

[1] See also Ong R, *Recognition of the right to privacy on the Internet in China,* International Data Privacy Law, 2019, Vol. 1, No. 3.

анализа и достижения всеобъемлющего подхода концепция защиты частной жизни также будет разработана под названием “режим защиты данных”.

Если изъяснятся четко и кратко то, Китай до недавних времен не нес никаких международных обязательств в отношении защиты данных. Несмотря на то, что АТЭС является “экономикой-членом”, рамки конфиденциальности АТЭС ни в коем случае не являются обязательными для подписавших ее государств. На самом деле следует иметь в виду, что АТЭС - это организация государств, которая не имеет Конституции или договора о ее создании, но действует на основе консенсуса и берет на себя обязательства на добровольной основе, претендуя на то, чтобы быть “единственной межправительственной группировкой в мире, действующей на основе необязательных обязательств»[1]. «Соглашения» АТЭС, такие как его рамки конфиденциальности, не имеют никакого правового статуса и лучше всего воспринимаются как согласованные устремления, подкрепленные консенсусными обязательствами сотрудничать.

Что касается других международных документов по защите данных, то Китай входит в число стран, с которыми ОЭСР “тесно сотрудничает” в рамках своей деятельности, в то время как Китай также входит в число стран, не являющихся членами Совета Европы, куда Совет Европы направляет приглашения подписать и ратифицировать соответствующие конвенции (в их числе и его Конвенция о защите данных), однако до сегодняшнего дня Китай официально не ратифицировал и даже не подписал их в рамках предмета защиты данных. Следовательно, с учетом вышеизложенного и в отсутствие какой - либо другой международной схемы защиты данных Китай до сегодняшнего дня, как представляется, свободен от каких-либо международных обязательств по защите данных.

[1] Greenleaf G, *The APEC privacy initiative: 'OECD Lite' for the Asia-Pacific?* Privacy Laws & Business, Vol. 71, 2020, 16-18.

Как отмечалось выше, в Китае нет всеобъемлющего Закона «О защите данных». Вместо этого за последние годы был принят ряд отраслевых законов, каждый из которых имеет различный правовой статус, причем ни один из них не относится исключительно к предмету защиты данных, а скорее включает в свои тексты некоторые конкретные положения о защите данных. В целом этот свод законов можно было бы объединить, чтобы сформулировать «кумулятивный» эффект защиты данных. Кроме того, частная жизнь защищена косвенно, как часть человеческого достоинства, в конституции Китая и в его основном гражданском праве. По причинам, описанным выше, ни один из этих следов защиты данных и двойников не может быть воспринят как формирующий режим защиты данных. Однако каждый из них будет подробно проанализирован в последующем анализе, чтобы получить полную картину и иметь возможность оценить точные размеры кумулятивного эффекта, обсуждаемого в отношении защиты данных в Китае. Следует отметить, что весь приведенный ниже анализ основан на вторичных источниках. Ниже приведены нормативные акты, которых прямо или косвенно касается информационная безопасность, и которые до 2020 действовали в КНР.

Нынешняя Конституция Китая была принята 5-м Всекитайским собранием народных представителей 4 декабря 1982 года и впоследствии была изменена в 1988, 1993, 1999 и 2004 годах. Конституция Китая не должна восприниматься так же, как западные Конституции. Например, в его статье 35 говорится, что « граждане Народной Республики в Китае пользуются свободой слова, печати, собраний, ассоциаций, шествий и демонстраций”. Кроме того, китайским судам не разрешается признавать закон недействительным на том основании, что он нарушает Конституцию, или применять его положения в интересах отдельных лиц; фактически его Конституция была определена как “не подлежащая судебному разбирательству”.

С другой стороны, следует отметить, что его поправка в 2004 году прямо касалась прав человека и обязательства государства “уважать и сохранять” права человека (Статья 33.3).

В Конституции Китая нет положений, связанных с защитой данных. Конфиденциальность упоминается только один раз, в частности, в отношении “свободы и конфиденциальности переписки” (Статья 40). В то время как утверждается, что «Конституция устанавливает право человека на достоинство, которое в соответствии с соответствующими нормами далее интерпретируется как включающее право на неприкосновенность частной жизни», это не отражено в фактическом тексте Конституции (соответствующая формулировка в ее статье 38: «личное достоинство граждан Китайской Народной Республики неприкосновенно. Оскорбление, клевета, ложное обвинение или подстава, направленные против граждан любыми средствами, запрещены»).

Наконец, что касается прецедентного права, то, по-видимому, единственный случай до 2014 года, связанный с защитой конституционных прав и, возможно, имеющий некоторое отношение к настоящему докладу, поскольку он касался кражи личных данных, был позже отменен Верховным народным судом. Следовательно, очень мало может быть выведено о каком-либо режиме защиты данных или даже защиты частной жизни в Китае из его Конституции.

Развивая Конституционный подход Китая, возможно, полезно учитывать, что частная жизнь воспринимается средним китайским человеком не так, как на Западе. На самом деле было отмечено, что “конфиденциальность остается странным понятием для многих в Китае, и право на частную жизнь не является неотъемлемой частью прав человека. Люди не имели четкого представления о том, как отличить постыдную тайну (на кит. Insi) от личной жизни (на кит. Insi). Эти два слова очень часто употреблялись попеременно, ибо произношение их почти то же самое за исключением небольшой разницы тонов.

Это, вероятно, объясняет, почему, изучая право на неприкосновенность частной жизни, ученые стремятся прояснить его элементы и сферу охвата. В этом есть доказательства влияния западной юридической науки", китайские граждане, закон и суды продолжают в основном ассоциировать право на частную жизнь (ни слова о защите данных) с правом на репутацию и достоинство.

К 2012 году в законодательстве Китая произошли некоторые изменения. В частности, речь идет о решении SCNPC 2012 года.

Постоянный комитет Всекитайского собрания народных представителей (ВСНП/SC-NPC), как уже отмечалось, является вторым по значимости законодательным органом Китая, и его решения фактически представляют собой законодательство. В 2012 году комитет опубликовал свое «решение о защите информации в Интернете ("решение SC-NPC 2012 года»). Это решение до сих пор является законом самого высокого уровня в Китае, специально посвященным вопросам защиты данных. Поскольку все другие соответствующие законодательные акты, такие как инициативы Министерства промышленности и информационных технологий, которые обсуждаются непосредственно ниже, должны соответствовать ему, а также поскольку это решение является единственным китайским правовым документом по защите данных, который также применяется к государственному сектору, оно считается де - факто стандартом защиты данных в Китае.

Решение SC-NPC состоит всего из 12 статей и направлено на защиту «электронной информации» в соответствии со статьей 1, что фактически означает, что в некоторых положениях ее защита может быть шире, чем интернет, только в соответствии с ее названием. Защита личной неприкосновенности прямо упоминается также в его статье 1. Адресатами решения являются «интернет-провайдеры, а так же другие предприятия и учреждения, которые собирают или используют личную электронную информацию граждан в ходе своей деятельности». Они «должны соблюдать

принципы законности, четко указывать цель, методы и объем сбора и использования информации, а также получать согласие от лица, данные которого собираются. Они не могут нарушать положения законов и нормативных актов и соглашения между обеими сторонами при сборе или использовании информации» (Статья 2). Конфиденциальность и безопасность обработки данных защищены в равной степени (соответственно в статьях 3 и 4). «Реальная идентификационная информация» запрашивается всеми поставщиками сетевых услуг при предоставлении онлайновых или телекоммуникационных услуг (статья 6). Субъектам данных предоставляется право при обнаружении нарушения их прав просить контролеров данных «удалить информацию", "прекратить нарушение" или» сообщить в контролирующие органы « (статьи 8 и 9).

Если бы решение SC-NPC 2012 года было оценено в соответствии с моделью защиты данных ЕС, то его недостатки стали бы легко очевидными в том смысле, что ему не хватает сферы охвата (только интернет), механизма правоприменения, основных прав субъектов данных, а также его принципиальной установки (их список не включает все принципы подхода ЕС к защите данных). Однако если рассматривать это решение как первую попытку создания всеобъемлющего режима защиты данных, то оно действительно имеет определенные достоинства, главным образом в виде основных элементов защиты данных, которые можно найти в его тексте. Кроме того, его высокоуровневое происхождение означает, что он устанавливает фактический стандарт в области обработки персональных данных, связанных с интернетом. Другие китайские агентства быстро подхватили это новое развитие событий: фактически ключевая терминология решения (то есть общие принципы, изложенные в статье 2) была принята в других законодательных актах, последовавших за ним, таких как правила MIIT 2013 года и поправки 2013 года к китайскому закону о потребителях.

1 июля 2015 года на 15-м заседании Постоянного комитета двенадцатого Всекитайского собрания народных представителей был принят новый закон Китайской Народной Республики «О национальной безопасности»[1]. Статья 25 Закона «О национальной безопасности» гласит: «Государство создает систему Интернет-и информационной безопасности, укрепляет свои возможности по защите информационной безопасности, усиливает исследования, разработки и применение инноваций в области интернета и информационных технологий, а также делает основные технологии интернета и информации, ключевые инфраструктуры, информационные системы и данные в ключевых секторах безопасными и контролируемыми; укрепляет управление киберпространством, предотвращать, пресекает и наказывает киберпреступные действия, такие как кибератаки, киберпреступления, киберкражи и распространение незаконной и вредной информации, а также защищает национальный суверенитет, безопасность и интересы развития киберпространства». Закон впервые конкретизирует понятие «суверенитет киберпространства» на правовом уровне, причем суверенитет киберпространства может трактоваться как воплощение, расширение и отражение государственного суверенитета.

Далее обратимся к нововведениям, которые имели место быть буквально «на днях».

В октябре 2020 года Китай обнародовал свой законопроект о защите персональных данных. После обнародования этот закон станет первым всеобъемлющим сводом законов КНР о защите персональных данных.

Долгожданный проект закона Китайской Народной Республики О защите персональной информации (далее - «проект пипл») был выпущен для

[1] National security law of the People’s Republic of China. http://www.npc.gov.cn/npc/xinwen/2015-07/07/content_1941161.html [2021-9-17].

публичных консультаций 21 октября 2020 года. Консультационное окно закрылось 19 ноября 2020 года.

PIPL, как только он будет обнародован, станет первым всеобъемлющим сводом законов Китая, направленных на решение проблем с утечками персональных данных и хакерскими атаками, распространенными в стране. С быстрым ростом индустрии больших данных и огромным количеством пользователей сети в Китае PIPL, как ожидается, будет играть важную роль в регулировании обработки персональных данных и борьбе с неправильным использованием собранных данных.

В настоящее время закон Китая о кибербезопасности (“CSL”), вступивший в силу в 2017 году, регулирует защиту личной информации. CSL фокусируется на защите информации в киберпространстве, защите “критической информационной инфраструктуры” и регулировании “сетевых операторов”. PIPL будет более всеобъемлющим законом, который регулирует больше аспектов защиты личной информации.

Проект «пипл» состоит в общей сложности из восьми глав и 70 статей. Различные аспекты проекта PIPL напоминают GDPR ЕС. Среди прочего, проект PIPL устанавливает принципы защиты данных, конкретные правила обработки как “личной информации”, так и “конфиденциальной личной информации”, права отдельных субъектов данных, а также штрафы за нарушения.

Ниже приводится краткое изложение того, что считается ключевыми моментами проекта PIPL:

- экстерриториальное применение PIPL
- больше оснований, на которых допускается обработка личной информации
- больше прав и защит, предоставляемых физическим лицам

- регулирование роли “обработчиков личной информации”
- локализация данных и трансграничная передача личной информации
- штрафы до 50 миллионов юаней (7,5 миллиона долларов США) или 5% годового оборота.

К сожалению, в проекте нет указания на то, какой из них устанавливает нижний или верхний предел. Очевидно, что это важный вопрос, который нуждается в скорейшем прояснении.

Законы КНР, как правило, не имеют экстерриториального действия. Однако проект PIPL будет применяться к обработке персональных данных за пределами границ Китая, если:

1. Информация, о которой идет речь, относится к физическому лицу(лицам) в пределах границ Китая;
2. Обработка такой информации подпадает под одно из следующих обстоятельств:

    - если целью обработки личной информации является предоставление товаров или услуг физическим лицам в пределах границ Китая;
    - если целью является анализ или оценка деятельности физических лиц в пределах границ Китая;
    - в соответствии с требованиями или положениями законов или административных регламентов.

Утверждение об экстерриториальном применении проекта PIPL тесно связано с GDPR ЕС. Эффективность любой экстерриториальной юрисдикции проекта «пипл», вероятно, придется рассматривать в свете соответствующих правил и процедур правоприменения. В качестве разумной практики с целью соблюдения PIPL бизнес-учреждение или организация, не базирующиеся в КНР, которые имеют присутствие в Китае или затрагивают персональные

данные лиц, находящихся на территории Китая, должны назначить сотрудника по защите данных или представителя в КНР для надзора за обработкой персональных данных.

В соответствии с CSL согласие физического лица является единственным основанием, на котором личная информация может быть собрана и обработана. Личная информация может быть собрана только в том случае, если соответствующее лицо проинформировано и согласилось с целями и объемом сбора. Таким образом, CSL довольно узок.

Ожидается, что проект PIPL будет одобрен, поскольку он предоставляет альтернативные правовые основы для сбора и обработки личной информации. Помимо получения согласия, личная информация может быть собрана и обработана в любом из следующих обстоятельств:

- когда это необходимо для заключения или исполнения договора, стороной которого является физическое лицо;
- когда это необходимо для выполнения обязанностей или обязательств, предусмотренных законом;
- когда это необходимо для реагирования на внезапные инциденты в области общественного здравоохранения или защиты жизни, здоровья и имущественной безопасности физических лиц в чрезвычайных ситуациях;
- обработки в пределах разумности личной информации в новостях и изучения общественного мнения в общественных интересах или других обстоятельств, предусмотренных законом или административными регламентами.

Хотя в настоящее время предлагается больше правовых основ, большинство из этих правовых основ, по-видимому, не оказывают большой помощи предприятиям или организациям частного сектора. Наиболее

примечательно, что в отличие от GDPR, проект PIPL не допускает сбора или обработки личной информации на основе “законного интереса”, что является наиболее гибкой основой, доступной в соответствии с GDPR.

Если коммерческое учреждение или организация или “обработчик информации о данных” склонны полагаться на основание “законного интереса” для сбора и обработки персональных данных в соответствии с GDPR, им необходимо будет быть осторожными, поскольку им придется рассмотреть вопрос о том, можно ли полагаться на какие-либо альтернативные основания, указанные в проекте PIPL. В противном случае информированное согласие индивида все равно должно быть получено.

Правила, содержащиеся в проекте «пипл», регулирующие согласие, обеспечивают большую защиту отдельным лицам. Как правило, согласие в соответствии с проектом «пипл» должно быть хорошо информированным, добровольным и ясным. Он может быть отозван физическим лицом по своему желанию и должен быть получен от него в случае любого изменения цели обработки, метода обработки и вида обрабатываемой информации. Прямо предусмотрено, что отказ или отзыв согласия не может быть причиной, по которой предоставление продуктов или услуг должно быть отказано физическому лицу.

Необходимость получения согласия от физических лиц распространяется также на использование общедоступной личной информации в зависимости от того, как такая информация использовалась в то время, когда она впервые стала общедоступной. Если предполагаемое использование общедоступной информации не имеет разумного отношения к ее первоначальным целям, необходимо будет получить согласие.

Отдельное согласие должно быть получено в отношении «конфиденциальной личной информации». «Конфиденциальная личная

информация» в соответствии с проектом PIPL описывается как информация, которая может привести к дискриминации человека или нанести ущерб физической или имущественной безопасности человека в случае утечки или незаконного использования. В отличие от GDPR, который устанавливает исчерпывающий перечень специальных категорий персональных данных, список “конфиденциальной личной информации”, приведенный в проекте PIPL, короче соответствующего списка в соответствии с GDPR и не является исчерпывающим. Он может охватывать более широкий объем личной информации по сравнению с GDPR, в зависимости от того, насколько строго или свободно будет интерпретироваться это определение “конфиденциальной личной информации”. При разработке политики обработки персональных данных обработчики персональных данных должны быть готовы тщательно изучить виды обрабатываемой личной информации с точки зрения потенциальных последствий в случае нарушения безопасности данных.

Имея ввиду юрисдикцию будущего закона, следует принять во внимание, что законопроект включает в себя метод «юрисдикции длинной руки», широко применяемый в правовой практике Америки[1]. Таким образом, деятельность китайский фирм будет находиться под влиянием будущего закона. Фирмы будут загнаны в условия, при которых необходимо создать подразделения или привлечь специалистов, отвечающих за данные задачи.

Одновременно с этим для законного экспорта личных данных локальным организациям будет нужно реализовать по крайней мере одно из таких действий как получение оценки безопасности Национального департамента кибербезопасности и информатизации, получение специальной

[1]Новый законопроект «О защите персональных данных» — возможен ли баланс в кибериндустрии?[Электронный ресурс]//.URL:https://zakon.ru/blog/2020/12/01/novyj_zakonoproekt_o_zaschite_personalnyh_dannyh_-_vozmozhen_li_balans_v_kiberindustrii

сертификации (в установленной законом форме) профессиональной организации.

Операторы, работающие с информационными потоками и обрабатывающие личные данные граждан, и объем работы которых достигает установленных пределов, обязаны пройти процедуру проверки безопасности. В том случае, если оператор был связан с иностранными компаниями или лицами и передавал им персональные данные по каким-либо причинам, надзор за ними будет осуществляться в более строгой мере. Требования к таким операторам в области сбора, обработки и передачи информации вырастут[1].

Если в Китае какие-либо иностранные компании или граждане нарушают государственную безопасность и вторгаются в личные границы жителей страны их включают в специальный черный список компаний и физических лиц, который находится в открытом доступе для всех граждан страны. Такие компании или лица могут быть ограничены частично или полностью в осуществлении своих функций и приговорены к ответственности.

Таким образом, важно не нарушать не только из-за высокой стоимости наказания, но и из-за выгодности следования законодательству.

Говоря об информационно-правовом опыте Республики Казахстан в сфере выработки нормативного механизма защиты персональных данных, следует отметить, что правовой основой развития института защиты персональных данных послужил Закон Республики Казахстан «О персональных данных и их защите». Означенный закон характеризует понятие персональных данных как сведений, относящихся к определенному или определяемому на их основании субъекту персональных данных,

[1] Новый законопроект «О защите персональных данных» — возможен ли баланс в кибериндустрии? [Электронный ресурс] //. URL: https://zakon.ru/blog/2020/12/01/novyj_zakonoproekt_o_zaschite_personalnyh_dannyh_-_vozmozhen_li_balans_v_kiberindustrii

зафиксированные на электронном, бумажном или ином носителе в материальной форме. Некоторые авторы критикуют данную дефиницию, поскольку она не позволяет установить исчерпывающий перечень сведений, относящихся к персональным данным[1]. Как представляется автору настоящей работы, приведенная норма-дефиниция является вполне обоснованной, поскольку не допускает необоснованного ограничения объектов персональных данный с учетом интенсивного развития информационных технологий. Тем, не менее, основной закон в области защиты информации помимо этого содержит ряд пробельных положений. Так, например, Закон Республики Казахстан «О персональных данных и их защите» не содержит положений об уполномоченном органе, осуществляющем функции по защите персональных данных. Понятие обработки персональных данных в исследуемом законе гораздо уже аналогичного понятия, содержащегося в иных нормативных актах[2].

Итак, стратегический план по улучшению степени защиты персональных данных окажет непосредственное влияние не только на деятельность компаний и физических лиц, но и станет новым испытанием в области баланса интересов в глобальной сети Интернет.

2.2. COVID-19 и применимое право к транснациональным персональным данным человека.

Недавняя вспышка COVID-19 подтолкнула напряженность защиты персональных данных в транснациональном контексте к апогею. Это происходит потому, что COVID-19 быстро распространяется вместе с международными поездками людей. Многие страны требуют, чтобы международные

[1] Максутов Б. М. Правовой механизм защиты персональных данных в Казахстане на основе общего регламента по защите персональных данных (GDPR) // INTERNATIONAL SCIENTIFIC REVIEW OF THE PROBLEMS OF LAW, SOCIOLOGY AND POLITICAL SCIENCE. 2019. С. 29.

[2] Например, в Директиве 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 г.

путешественники раскрывали свою личную информацию, такую как имя, пол, дата рождения, история путешествий, цель поездки и место жительства, и соответственно вводят карантинные требования . В конце марта 2020 года китайские СМИ широко сообщили об австралийской даме китайского происхождения, которая нарушила требование домашнего карантина, пробежав трусцой без маски в жилом комплексе, где она временно жила в Пекине[1]. Китайский полицейский потребовал, чтобы женщина осталась дома. В свою очередь, дама отказалась и заявила, что подверглась насилию со стороны полицейского. Китайские СМИ опубликовали ее фотографию, ее возраст, информацию о рейсе, ее имя, национальность, ее временный домашний адрес в Пекине, китайский и австралийский университеты, которые она окончила, и годы ее окончания, ее трудовую историю и должности, ее нынешнего работодателя, даже размер её зарплаты. Ее работодателем была китайская дочерняя компания немецкого фармацевтического гиганта Bayer. Bayer China среагировали довольно таки оперативно и за несколько дней оформили заявление, уволив женщину за нарушение Китайского карантинного требования.

Поскольку китайская её виза была спонсирована работодателем, китайское правительство отозвало ее визу и депортировало ее после того, как Байер расторг с ней трудовой договор. Очевидно, женщина нарушила обязательную самоизоляцию COVID-19 регулированный в Китае. Ее поведение угрожало общественному здоровью и должно было быть осуждено. Однако оправдывает ли ее преступление разглашение ее подробной личной информации в Интернете?

Исходя из обнародованной информации, личность её можно легко установить: она гражданка Австралии, и она прибыла в Китай всего за один день до того, как произошел инцидент. Поэтому она не в состоянии получить привычное

---

[1] An Australian Woman Breached Coronavirus Quarantine in Beijing to Go for a Jog—And Lost Her Job, https://edition.cnn.com/2020/03/20/asia/beijing-coronavirus-woman-fired-intl-hnk/index.html (дата обращения: 01.04.2021).

место жительства в Китае за такой короткий срок. Она была старшим директором, работающим в Bayer China, которая принадлежала Bayer Germany, хотя в новостях не указывалось, была ли она нанята Bayer Germany, и обрабатывалась ли ее личная информация о работе в Германии.

К сожалению, данный случай не является единичным. Это типично и демонстрирует напряженность между предотвращением COVID-19 и защитой транснациональных персональных данных: какой закон должен применяться к персональным данным международного путешественника, нарушившего местный закон о карантине?

Защита персональных данных в транснациональном контексте важна и необходима. Это связано с тем, что в современном обществе, где люди часто путешествуют через границы, такие технологии, как Интернет и облако, по своей сути являются транснациональными, и поставщики онлайн-услуг также активно делают свои услуги доступными по всему миру[1]. Национальные регулирующие органы также стали более серьезно относиться к защите персональных данных в транснациональном контексте. ЕС ввел в действие Общее положение о защите данных. Правительство штата Калифорния приняло Калифорнийский закон о неприкосновенности частной жизни потребителей. Китай включил право на персональные данные в Общие нормы гражданского права Китая[2].

Австралия уверенно создает право на потребительские данные. Однако содержание национальных законов о защите персональных данных не совпадает. Например, китайские СМИ опубликовали информацию о занятости (как нынешних, так и прошлых работодателей) и образовании международного путешественника, нарушившего карантинное требование COVID-19. В ЕС такая личная информация будет защищена в соответствии с GDPR, Заявлением об

---

[1] Georg Haibach, *Cloud Computing and European Union Private International Law,* 11 J. PRIV. INT. LAW 252– 266, 253–54 (2015)

[2] General Rules of the Civil Law of China [Minfa Zongze], promulgated on 15 March 2017 and effective on 1 October 2017, http://www.court.gov.cn/zixun-xiangqing-37832.html (дата обрпщения: 07.07.2021).

обработке персональных данных в контексте вспышки COVID-19, принятым Европейской службой данных.

В Австралии некоторые штаты могут разглашать информацию о рейсах и местах, где побывал международный путешественник, зараженный COVID-19, но его или ее полное имя, должность и зарплата, а также информация об образовании никогда не разглашаются, если только эта

информация не необходима для уменьшения или предотвращения серьезной и неминуемой угрозы здоровью австралийской общественности.

Различные национальные меры по защите персональных данных в борьбе с COVID-19 демонстрируют необходимость определения применимого законодательства к транснациональным персональным данным. В соответствии с коллизионным правом, при поиске lex causae выделяют три этапа: охарактеризовать вопрос в одну из установленных классификаций выбора права путем определения природы предмета, выбрать норму коллизионного права, которая устанавливает связующий фактор для рассматриваемого вопроса, и определить систему права, которая связана связующим фактором, найденным на втором этапе, с вопросом, характеризуемым на первом этапе.

Существуют ценные национальные исследования или сравнительные исследования, изучающие защиту персональных данных. Однако в небольшой коллизионной литературе сравнивается как Китай, США и ЕС будут характеризовать право на персональные данные, какие связующие факторы они будут учитывать и какой закон они в конечном итоге будут применять для защиты персональных данных. Эти вопросы особенно важны в контексте COVID-19, где государства строго следят за международными путешественниками.

Утверждается, что Китай, США и ЕС характеризуют право на персональные данные совершенно по-разному. ЕС выделяет его как фундаментальное право человека, США считают его гражданской свободой, а Китай считает право на персональные данные правом личности. Данные выводы так же можно сделать исходя из характеристики защиты прав о персональных данных человека в Китае, учитывая опыт предыдущего параграфа. В данном пункте целесообразно

проанализировать материальное право защиты персональных данных в США, ЕС и Китае. Устанавливается тенденция того, что глобальная тенденция материального права смещается от американизации к деамериканизации.

Природа права на персональные данные по-разному характеризуется в ЕС, США и Китае. Из-за обязательного характера закона о защите персональных данных и связующего фактора, ведущего к праву суда, применимое право для транснациональных персональных данных зависит от гонки в суды или регулирующие органы.

Тем временем внутренние законы о защите персональных данных по существу переживают движение деамериканизации. Необходимо пересмотреть отношения между корпоративными гигантами интернет-данных и государствами. Общепринятая мудрость заключается в том, что Интернет - компании действуют лишь в небольшой степени в тени государственного права. Эти гиганты должны соблюдать закон своего места жительства, который часто является законом США. Тенденция развития регулирования интернет-индустрии (особенно информационной) перешла от американизации к деамериканизации. Это было вызвано сочетанием законодательных и не законодательных подходов в ЕС и Китае. Знаковые примеры включают принятие GDPR в ЕС, призыв Крайстчерча, инициированный Новой Зеландией и Францией, а так же запрет Huawei и онлайн-пропаганду COVID-19, которая разделяет Китай и США/ЕС.

Профессор Джек М. Балкин указывает: «В настоящее время Интернет в основном управляется ценностями наименее цензурного режима—режима Соединенных Штатов»[1]. С точки зрения коллизионного права это явление может быть объяснено значимостью права Домицилия. Основными глобальными интернет-игроками являются американские компании и отраслевые ассоциации, зарегистрированные в США. Среди десяти крупнейших интернет-компаний мира

[1] Jack M. Balkin, Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation, 51 U.C. DAVIS L. REV. 1149, 1206 (2018).

шесть — это американские компании: Amazon, Google, Facebook, Netflix, Booking и eBay.

Домициль компании данных является значительным, иногда определяющим, чтобы определить закон, который будет применяться для защиты персональных данных, собранных компанией[1]. Американская среда регулирования данных характеризуется свободой слова, отраслевым саморегулированием, декретами о согласии Федеральной торговой комиссии и слабыми правилами конфиденциальности потребителей. Домициль компании также важен для целей признания и приведения в исполнение судебных решений. Следовательно, это характеризуется обеспокоенностью тем, может ли внутренний закон о защите персональных данных соблюдаться в других юрисдикциях.

Например, Yahoo обвинили в пособничестве фашистам. Многонациональная компания Licra, выступающая против расизма, подала заявление в суд на Yahoo по причине того, что те выставили на продажу некоторые товары с нацисткой символикой, а в онлайн-конференциях участвуют неонацисты. Управляющие Licra сделали упор на том, что среди таких товаров было около восьмисот наименований, имеющих отношения к нацистской Германии. Один из главных экспонатов – нож Гитлера. Упор компанией Licra был сделан на том, что нацистские символы активно продвигались и не скрывались. Популярным хештегом для поиска такого рода товаров стал #nazi.

Yahoo! относится к юрисдикции в США и неудивительно, что он обратился в окружной суд США и успешно добился решения, в котором было объявлено, что французское решение не является признанным и подлежащим исполнению в нарушение Первой поправки к Конституции США. Хотя решение окружного суда было отменено на апелляционном уровне на основании отсутствия личной юрисдикции в отношении LICRA & UEJF и “зрелости” исполнительного иска, тем не менее оно демонстрирует, что Первая поправка к Конституции США

[1] Uta kohl, jurisdiction and the internet: regulatory competence over online activity 201 (2007).

потенциально может быть использована для защиты сайтов, зарегистрированных в США, от исполнения иностранных судебных решений.

Аналогичная ситуация произошла между Корпорацией Google Inc v Equustek Solutions Inc , Google не было необходимости в канадском суде, чтобы заблокировать сайты, нарушающие канадское законодательство[1]. Google является еще одной компанией, имеющей постоянное место жительства в США. Следовательно по аналогии он получил решение в своем родном суде, которое сделало канадское решение неисполнимым. Кроме того, Закон США Об обеспечении защиты прочного и устоявшегося конституционного наследия (далее "Закон о РЕЧИ 2010") прямо запрещает признание и приведение в исполнение иностранных судебных решений о диффамации в отношении онлайн-провайдеров, если только ответчик не был бы привлечен к ответственности в соответствии с законодательством США[2].

Материальное право в области защиты персональных данных и в целом международные нормативные акты переходят от американизации к деамериканизации. Двумя основными драйверами являются ЕС и Китай. Несмотря на критику, GDPR может начать европеизацию законодательства о защите данных и символизирует глобальную тенденцию деамериканизации правил индустрии данных.

ЕС гармонизирует закон о защите данных двумя способами. Первый - внутри ЕС. Директива ЕС о защите данных позволяет государствам-членам применять свое собственное законодательство. В отличие от этого, GDPR установил более гармонизированную структуру благодаря своему прямому применению в государствах-членах ЕС[3].

---

[1] Equustek Solutions Inc v Jack (2014) 374 DLR (4th) 537; Equustek Solutions Inc v Google Inc (2015) 386 DLR (4th) 224; see also Google Inc v Equustek Solutions Inc [2017] 1 SCR 824. Jennifer Daskal, Google Inc. v. Equustek Solutions Inc., 112 AM. J. INT. LAW 727, 727-33 (2018).

[2] SPEECH Act 2010, https://www.congress.gov/111/plaws/publ223/PLAW-111publ223.pdf (last visited November 9, 2019).

[3] Paul Lefebvre & Cecilia Lahaye, EU Data Protection and the Conflict of Laws: The Usual "Bag of Tricks" or a Fight Against the Evasion of the Law?, 84 DEF. COUNS. J. 1, 2 (2017).

Кроме того, учитывая длинную юрисдикцию, созданную GDPR, суды также могут быть склонны применять GDPR. По сравнению с Директивой об электронной коммерции, GDPR особенно актуален для защиты персональных данных в борьбе с COVID-19. Европейский совет по защите данных официально объявил, что GDPR применяется к обработке персональных данных в контексте COVID-19. При обработке персональных данных

компетентными органами здравоохранения и работодателями по причинам, представляющим существенный общественный интерес в области здравоохранения, нет необходимости полагаться на согласие физических лиц.

Во-вторых, координация материального права в области защиты персональных данных между членами ЕС и теми странами, которые не входят в ЕС, также осуществляется через решение Европейской комиссии, которое требует, чтобы государство, получающее данные из ЕС, вводило высокий стандарт закона о защите данных, эквивалентный ЕС[1].

Статья 45 GDPR предусматривает, что передача персональных данных за пределы ЕС осуществляется на основании решения Европейской комиссии об адекватности. Комиссия будет принимать во внимание три элемента при принятии решения:

– соблюдение прав и основных свобод человека, правомерность;

– наличие в международной компании или третьей стране действенного работающего учреждения, осуществляющего контроль, которое несло бы ответственность за следование правовым актам и законам о защите персональных данных;

– обязательства или какие-либо обязанности, которые взяли на себя международная компания и третья страна.

Решение «об адекватности», а именно о достаточности уровня защиты не является окончательным.

[1] Aaditya Mattoo & Joshua P. Meltzer, *International Data Flows and Privacy: The Conflict and Its Resolution*, 21 J. INT. ECON. LAW 769, 775–777 (2018).

Европейская комиссия должна проводить периодический обзор, по крайней мере, раз в четыре года, и следить за развитием событий в странах, получивших положительное решение об адекватности.

Помимо GDPR, еще одной важной глобальной попыткой ограничить влияние слабых интернет-правил является Призыв Крайстчерча. 15 марта 2019 года боевик напал на две мечети в Крайстчерче, Новая Зеландия[1]. Боевик в прямом эфире транслировал бойню в первой мечети на своей странице в Facebook. В результате терактов погиб 51 человек. Согласно параграфу 230 Закона «О приличиях в области коммуникаций (далее “CDA”)»: интернет-посредник, такой как Facebook, не несет гражданской ответственности, вызванной контентом третьих лиц.

Таким образом, применяя американское законодательство, Facebook не будет нести никакой ответственности за то, что боевик разрешил прямую трансляцию бойни в Интернете.

15 мая 2019 года премьер-министр Новой Зеландии Джасинда Арден, президент Франции Эммануэль Макрон и главы многих других государств и руководители технологических компаний приняли Призыв Крайстчерча[2]. Призыв направлен на то, чтобы «объединить страны и технологические компании в попытке положить конец возможности использования социальных сетей для организации и пропаганды терроризма и насильственного экстремизма”. Поставщики онлайн-услуг, включая Facebook, обязались принять прозрачные и конкретные меры для предотвращения загрузки террористического и насильственного экстремистского контента и прекратить его распространение на сервисах обмена контентом. В отличие от GDPR, призыв Крайстчерча не имеет

[1] Christchurch Shootings Mark ‘Unprecedented Act of Violence’, New Zealand Prime Minister Jacinda Ardern Says, https://www.abc.net.au/news/2019-03-15/christchurch-shootings-unprecedented-pm-jacinda- ardern-says/10904950 (дата обращения: 04.05.2021).

[2]Christchurch Call to Eliminate Terrorist & Violent Extremist Content Online https://www.christchurchcall.com/ (дата обращения: 04.05.2021).

обязательной силы. Тем не менее, она получила широкую поддержку в Океании и ЕС, и ее мягкий правовой характер может способствовать ее популярности в Европе.

К настоящему времени этот Призыв был подписан семнадцатью странами: от развивающихся стран, таких как Сенегал и Индия, до развитых стран, таких как Япония и Германия. Многие известные американские интернет-компании поддержали данный призыв.

В отличие от GDPR и других законодательных актов, Призыв Крайстчерча представляет собой не законодательный подход, который все чаще используется для получения согласия американских интернет-гигантов.

Важное различие между законодательным и не законодательным подходом заключается в том, что последний может обойти трудности приведения в исполнение иностранных судебных решений в соответствии с “речевым Актом» (speech act) в США. Это связано с тем, что промышленное соответствие воплощено в условиях предоставления услуг и может применяться во всем мире. В отличие от этого, решение суда может быть приведено в исполнение только в государстве, вынесшем решение.

Если он не распознается и не подлежит исполнению в государстве, к которому относится компания (например, в США), его эффективность ограничена. Его глобальное воздействие еще более ограничено недостаточным международным механизмом признания и приведения в исполнение судебных решений.

Возвращаясь к Китаю, целесообразно отметить, что Китай является еще одним сильным сторонником деамериканизации регулирования индустрии данных. Он делает это по причинам, очень отличным от ЕС. ЕС продвигает деамериканизацию, потому что считает защиту персональных данных фундаментальным правом человека, а защиту невмешательства США-недостаточной. Для Китая главной движущей силой деамериканизации является национальная безопасность. Это стремление было усилено двумя недавними инцидентами.

Первый - это запрет Huawei в США[1]. Huawei является ведущим китайским производителем 5-G и вторым по величине производителем смартфонов в мире.

16 мая 2019 года президент Дональд Трамп добавил Huawei в черный список США и запретил американским компаниям вести с ними бизнес без предварительного получения одобрения правительства США на утверждение о том, что Huawei представляет “угрозы информационным и коммуникационным технологиям и услугам в США[2]. Из-за запрета компании, прекратившие поставки Huawei, включают в себя не только американские компании, такие как Google и Intel, но и неамериканские компании, включая британскую ARM УКС и Vodafone, Германия Инфинеон, и японская компания KDDI и Docomo. Эти компании имеют производственные линии в США и поэтому обеспокоены санкциями США в случае их несоблюдения. Хотя запрет Huawei был издан правительством США, он привел к широкому эффекту снежного кома, который в значительной степени исключил Huawei из глобальной цепочки поставок.

Ранее претензии на цифровой суверенитет в основном продвигались такими государствами, как Китай и Россия, а не частными технологическими компаниями. Исходя из этого, думается, что Китай больше заботится о национальной безопасности, чем о частных коммерческих интересах. Ярким примером является Закон Китая о кибербезопасности 2017 года, направленный на “защиту кибербезопасности, защиту суверенитета киберпространства и национальной безопасности”[3]. Однако Запрет Huawei может кристаллизовать частные компании в неамериканских союзниках, чтобы перейти к кампаниям по цифровому

---

[1] Sean Keane, Huawei Ban: Full Timeline as It Posts Smallest Profit Increases in 3 Years, https://www.cnet.com/news/huawei-ban-full-timeline-us-government-china-trump-security-threat-p40/ (дата обращения 01.04.2020).

[2] Sonam Sheth, Trump Declares a National Emergency, Which Could Set Up a Huge Blow to China’s Huawei, https://www.businessinsider.com.au/trump-national-emergency-china-huawei-2019-5, (last visited November 9, 2019)

[3] Cybersecurity Law of the People's Republic of China [Zhonghua Renmin Gongheguo Wangluo Anquan Fa], as adopted at the 24th Session of the Standing Committee of the Twelfth National People's Congress of the People's Republic of China on November 7, 2016, Art. 1.

суверенитету. Соединенные Штаты преподают им яркий урок: даже если они зарегистрированы за пределами США, они все еще подчиняются американскому законодательству, полагаясь на глобальную цепочку поставок, в которой доминируют американские компании и отраслевые ассоциации.

Таким образом, компания Huawei запрет будет способствовать де-американизации отраслевых нормативных актов сведения.

Второй инцидент - это глобальная пандемия COVID-19. Как обсуждалось выше «Уведомление о защите Персональных данных» (the Notification on Protecting Personal Information and Using Big Data to Support Joint Prevention and Control of Disease) является обязательным законом и должны применяться к международным путешественникам в Китае[1]. Это уведомление предусматривает, что все населенные пункты и департаменты должны придавать большое значение защите личной информации, за исключением тех учреждений, которые уполномочены Департаментом здравоохранения и санитарии Государственного совета в соответствии с Законом Китая о кибербезопасности, Законом о профилактике инфекционных заболеваний и борьбе с ними и Правилами о чрезвычайных ситуациях в области общественного здравоохранения. Ни одно другое подразделение или физическое лицо не может использовать личную информацию на основаниях профилактики эпидемий и борьбы с ними или профилактики заболеваний без согласия собираемого лица.

В тех случаях, когда законы и административные регламенты предусматривают иное, они применяются соответствующим образом:

1. Сбор персональных данных, необходимых для совместного предотвращения и контроля, должен осуществляться в соответствии с

[1] Notification on Protecting Personal Information and Using Big Data to Support Joint Prevention and Control of Disease, promulgated and effective on 4 February 2020 by the China Central Cyber Security and Informatization Commission.

национальным стандартом Правил безопасности персональных данных и придерживаться принципа минимального сбора.

2. Объект сбора ограничен ключевыми группами, такими как диагностированные лица, подозреваемые и близкие контакты в принципе, и, как правило, не нацелен на конкретные области для предотвращения фактической дискриминации в отношении конкретных географических групп.

3. Личная информация собранные для профилактики и борьбы с эпидемиями и профилактики заболеваний средства не должны использоваться для других целей.

4. Ни одно юридическое или физическое лицо не может раскрывать личную информацию, такую как имя, возраст, номер удостоверения личности, номер телефона, домашний адрес без согласия собираемого лица, за исключением совместной работы по защите от болезней и борьбе с ними.

5. Вся используемая личная информация должна быть десенсибилизирована и анонимизирована.

Китайские СМИ нарушили это Уведомление в случае COVID-19, потому что они опубликовали подробную личную информацию этой дамы без ее согласия. Сбор и обнародование ее информации не соответствовали принципу минимума, поскольку информация о ее работе, университете, который она окончила, и год ее окончания не имеют ничего общего с профилактикой и контролем заболеваний.

Согласно Уведомлению, департамент сетевой информации Китая должен оперативно бороться с незаконным сбором, использованием и разглашением личной информации, а также инцидентами, которые вызывают большую утечку персональных данных в соответствии с Китайским Законом о кибербезопасности и связанными с ним нормативными актами. Департамент полиции должен строго пресекать соответствующие преступления в соответствии с законом. Однако китайские власти ничего не сделали для исправления ситуации. Нарушение персональных данных, причиненное даме, обсуждается в первом абзаце настоящей статьи. Это вскрывает две проблемы.

Во-первых, по сравнению с GDPR ЕС механизм исполнения уведомления и других китайских законов о защите персональных данных значительно слабее. Нарушение GDPR может привести к штрафу в размере до 20 миллионов евро или до 4% от годового мирового оборота предыдущего финансового года, в зависимости от того, что больше[1]. Для сравнения, Закон Китая о кибербезопасности предусматривает, что нарушение персональных данных может привести к штрафу в десять раз превышающему незаконный доход; если нет незаконного дохода, штраф составляет менее 1 миллиона юаней.

Во-вторых, китайское законодательство о защите личной информации подчиняется национальным интересам Китая. Это особенно верно для онлайн-пропаганды COVID-19.

В январе и начале февраля 2020 года китайские СМИ широко сообщали, что распространение COVID-19 произошло из-за людей, которые незаконно продавали и ели диких животных[2]. Однако с распространением COVID-19 по всему миру китайские СМИ начали публиковать статьи, критикующие США как источник этой болезни с марта 2020 года[3]. В эту статью не входит обсуждение того, каково происхождение COVID-19 и кто должен нести ответственность. Дело в том, что резкий разрыв между Китаем и США относительно происхождения COVID-19 и соответствующей государственной ответственности еще больше подтолкнет Китай к жесткому контролю над онлайн-СМИ и интернет-компаниями, расположенными в Китае. Деамериканизация соответствует национальным интересам Китая.

---

[1] A list of fines and notices issued under the GDPR can be found at https://en.wikipedia.org/wiki/GDPR_fines_and_notices.

[2] Evidence is Confirmed that Virus is found at Huanan Fish Market, http://finance.sina.com.cn/7x24/2020-01- 23/doc-iihnzahk6049908.shtml. Lancet Published Chinese Scholar's Comment: the Relationship between Novel Coronavirus and Consumption Wild Animals, https://m.chinanews.com/wap/detail/zw/sh/2020/02- 12/9087971.shtml (дата обращения: 01.04.2021).

[3] E.g. Where does COVID-19 Come from? Chinese Academy of Sciences Published a Paper Telling You the "Truth", https://news.china.com/zw/news/13000776/20200301/37852321_all.html (дата обращения: 01.04.2021).

Таким образом, на каждом этапе определения применимого права для транснациональных персональных данных возникли три тенденции:

1. ЕС, США и Китай по-разному характеризуют право на персональные данные;

2. Распространенный односторонний подход к применимому праву исходит из того факта, что все три юрисдикции либо рассматривают закон о защите персональных данных как обязательный закон, либо принимают связующие факторы, ведущие к праву суда;

3. ЕС и Китай решительно выступают за деамериканизацию основных законов о защите данных.

Эти тенденции развиваются и взаимодействуют друг с другом. Их динамика двоякая.

На макроуровне тенденции согласуются друг с другом. Многогранная правовая природа права на защиту персональных данных способствует распространению одностороннего подхода к применимому праву.

Следовательно, деамериканизация была поддержана ЕС и Китаем. Все эти тенденции воплощают фундаментальную ценность и национальные интересы государств. Однако, поскольку эти ценности и интересы столь разнообразны, тенденции демонстрируют регулятивную конкуренцию между государствами в отношении персональных данных в транснациональных контекстах. Например, США чрезмерно ценят свободу слова, что объясняет принятие ими слабого регулирования данных и блокирование иностранных судебных решений, нарушающих Первую поправку к Конституции США. Напротив, в ЕС конфиденциальность персональных данных считается одним из основных прав человека. Поэтому неудивительно, что GDPR устанавливает широкую экстерриториальную юрисдикцию. Китайское управление данными исходит из национальной заинтересованности в использовании персональных данных в качестве ценного ресурса для развития индустрии данных и поддержания социальной стабильности. Поэтому Китай отличает право на персональные данные

от права на неприкосновенность частной жизни и поддерживает деамериканизацию.

На микроуровне, если мы рассмотрим каждую отдельную тенденцию, становится очевидным, что расходящиеся законы, принятые каждой юрисдикцией в этой тенденции, на самом деле несовместимы. Типичным примером является отраслевое саморегулирование персональных данных в США, которое вступает в противоречие с законами Китая и ЕС, которые явно настаивают на большем правительственном регулировании.

Однако в лагере деамериканизации различия, существующие в законах, принятых ЕС и Китаем, превышают нюансы. Поскольку содержание материальных законов, принятых США, ЕС и Китаем, настолько различно, координация материального права на региональном уровне решениями об адекватности GDPR фактически приводит к более широкому разрыву на международном уровне.

ГЛАВА 3. МЕЖДУНАРОДНО - ПРАВОВОЕ РЕГУЛИРОВАНИЕ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Еще во времени Великой Французской революции люди стали задумываться о своем праве на защиту персональных данных. В современных же источниках подобное право относилось ко Всеобщей декларации 1948 года выпуска. Согласно Всеобщей декларации, гражданин имеет право на защиту от вторжения в личную жизнь и право на ведение личной переписки с другими гражданами. Право на охрану персональных данных нарушаться без законных причин не могло ни организациями, ни государственными органами, ни другими гражданами. Декларация говорила о том, что информация о личности человека есть актив, имеющий ценность и подлежит обязательной охране со стороны государства.

США является первой страной, принявшей закон о защите персональных данных в 1974 году – «Закон о конфиденциальности». Закон запрещает разглашение информации из баз персональных данных (БД) без письменного разрешения гражданина на разглашение его данных, за исключением двенадцати установленных законом пунктов. Патриотический акт США – гарантия правовой защиты информации вступил в силу 26.10.2001.

В начале 21 века в Калифорнии был разработан и утвержден закон «О защите персональных данных», согласно которому компании, которые осуществляют реализацию продукции, должны в обязательном порядке уведомлять своих покупателей о распространении их данных (ФИО, номер страховки, телефон, данные банковских карт). Закон «О защите персональных данных» позволил найти слабые места в охране безопасности личных данных и дал пример для внедрения такого закона другим странам.

Теперь не только США планируют внедрить закон о защите персональных данных. Евросоюз планирует приступить к разработке новых законопроектов в данной сфере. И вначале 80-х в Советский Союз определял персональные данные граждан как независимую деятельность. Комитет

отечественных экспертов выделил ряд действий для защиты персональных данных от сбора, обработки, незаконного распространения. Данные действия были впервые подтверждены официально в Конвенции «О защите прав физических лиц при автоматизированной обработке персональных данных» (Конвенция № 108, согласно порядку в серии европейских контрактов)[1].

К концу 20 века Европейский парламент и Совет Европейского Союза приняли Директиву Европейского парламента от 24.10.1995 «О защите физических лиц при обработке персональных данных и свободном обращении с этими данными» на основе положений Договора о создании Европейского Союза.

Итак, проведенный анализ законодательных актов по защите персональных данных говорит нам о высокой значимости и необходимости решения данной проблемы не только для рядовых граждан, но и для государства в целом. Законы во многом похожи друг на друга и преследуют общую цель — гарантия защиты и юридическая поддержка граждан в решении проблем защиты конфиденциальных данных[2]. Особенно это стало актуальным в нынешних условиях резкого увеличения вычислительных мощностей, появления и роста кибертерроризма, угроз безопасности персональным данным граждан. На мой взгляд, наиболее точно и структурировано принципы защиты персональных данных описывает Директива 95/46/ЕС. В этом документе подробно описаны обязательства государства по защите персональных данных не только в законодательной и правовой сфере в целом, но и на уровне владельцев баз данных, а также права субъектов персональных данных.

---

[1] Баранов А.А. Права человека и защита персональных данных / А.А. Баранов, В.М. Брыжко, Ю.К. Базанов. [Электронный ресурс] // npr. URL: http://library.khpg.org/files/docs/Kn_L_.pdf (дата обращения: 23.06.2021).

[2] Абрамова А. Г. Современные проблемы осуществления защиты персональных данных в сети: основополагающие принципы защиты персональных данных // Регион и мир. 2020. № 4. С. 24-25.

Но, помимо этого, существует ряд исключений, когда может разглашать персональные данные (или наоборот – не разглашать).

На основании содержания Директивы 95/46/ЕС[1] в Европе были разработаны концепции законов о защите персональных данных. Помимо этого, Директива 95/46/ЕС стала основополагающим звеном в создании ФЗ №152 – ФЗ «О персональных данных» в России[2]. Все правовые акты в равной степени обязывают информировать субъектов персональных данных о работе с их данными (сбор, передача, обработка), а также обеспечивать их защиту в максимальной степени, чтобы предотвратить распространение этих данных несанкционированным способом.

В течение нескольких последних лет принимались различные нормативные и программные акты, обеспечивающие безопасность и защиту конфиденциальной информации от злоумышленников. Среди таких:

– Резолюция Европейского парламента «О защите прав гражданина в связи с прогрессом информатизации» от 1979 г., в которой закреплены важнейшие направления работы с информацией касательно стран Евросоюза;

– Европейская конвенция о защите от автоматического сбора, обработки и распространения данных о гражданах, разработанная Советом Европы в 1985 г.

Данные правовые документы действуют исключительно на территории стран Евросоюза и не распространяются на иные государства, в которых сфера защиты данных находится в подчинении их собственных законов.

Итак, анализ правовых источников показал, что законодательные акты в сфере работы с персональными данными носят общий характер и призваны защищать персональные данные, права граждан, чьи персональные данные

---

[1] Directive 95/46/ECof European parliament and Soviet dated 24 October 1995 “On protection of individuals when personal data processing and free float of this data» [Электронный ресурс] // npr. URL: 32.rsoc.ru/docs/32/Direktiva_95_46_ES__24.10.1995.doc. (дата обращения: 15.06.2021).

[2] Собрание законодательства Российской Федерации. – 2017. – № 31. – Ст. 4736.

подвергаются незаконному сбору, распространению и обработке, а также устанавливают обязательство по регистрации персональных данных в специальных базах данных. Более наглядно сравнение законодательных актов представлено в таблице 1.

Таблица 1 – Сравнение законодательных актов в сфере защиты персональных данных в США, России и Евросоюзе

Особенности законодательных актов	Страны		
	США	ЕС	Россия
База данных регистрации в государственном реестре владельцев	+	+	+
Специальный комитет по надзору	+	+	+
Группа, занимающаяся защитой персональных данных физических лиц	-	+	-
Реестр данных по обработке персональных данных	+	+	-
Обеспечение необходимого уровня защиты владельцами персональных данных	+	+	+
Необходимость согласия на обработку ПДН от субъекта данных	+	+	+
Предоставление данных незнакомым людям	+	-	-
Предоставление субъекту данных уведомления об обработке его данных	+	+	+
Передача информации о владельце ПДН субъекту ПДН	+	+	+
Субъект данных имеет право получить факты, информация о которых хранится в базе данных	+	+	+
Информация из базы данных не избыточная и соответствует целям, заявленным изначально	+	+	+
Публичность операций по обработке и хранению данных	+	+	-
Особенности обработки персональных данных в государственных или муниципальных информационных системах персональных данных	-	-	+
Возможность отказа в доступе к данным субъекту данных	-	-	+

Проведенные исследования показали, что существуют различия в обеспечении защиты персональных данных в законодательных актах России и стран Европейского Союза/США[1].

В законодательных актах России:

[1] Conflict of legislation on personal data of USA and the European Union [Электронный ресурс] // npr. URL: http://www.pdp.net.ua/stolknovenie-zakonodatelstv-o-personalnyx-dannyx-ssha-i-evropej-skogosouza http://www.pravo.vuzlib.net/book_z137_page_28.html. (дата обращения: 20.06.2021).

– требования определяются регулирующими органами (для обработки с помощью средств автоматизации);

– отсутствует привязка к характеру данных, технологиям обработки, затратам на обеспечение работы с информацией.

В законодательных актах Европейского Союза/США:

– учитывается характер персональных данных, прогнозируются действия нарушителей, разрабатываются технологии работы с информацией, система работы по причиненным убыткам имеет адекватную стоимость;

– подход к созданию систем защиты персональных данных максимально гибкий.

В настоящее время практически во всех штатах приняты законы о защите персональных данных. Наиболее развитыми в этом направлении являются США и Европейский Союз, которые имеют ряд законов, позволяющих обеспечить защиту этих граждан на должном уровне и урегулировать проблемы персональных данных в международных отношениях. Законодательные базы стран постсоветского пространства практически отсутствуют, за исключением России.

Конвенция 108 о защите физических лиц при автоматизированной обработке персональных данных, принятая Советом Европы, является единственным императивно обязывающим многосторонним соглашением в сфере защиты персональных данных. Конвенция 108 закладывает основы правового регулирования и предписывает сторонам включить в свое национальное законодательство меры, необходимые для обеспечения защиты прав человека в области обработки персональных данных.

Конвенция Совета Европы (СЕ) о защите данных 108 1981 года (с Дополнительным протоколом 2001 года) укрепляет свои позиции в качестве формирующегося глобального соглашения о конфиденциальности данных, но в его работе остаются нерешенные вопросы.

Важным событием, которое последует за собой долгосрочное значение, является то, что Европейский союз в настоящее время более решительно поддерживает Конвенцию 108 как глобальный договор о конфиденциальности. Одновременно с доработкой условий GDPR Совет ЕС принял в качестве одного из своих приоритетов на 2016 - 2017 годы в своих отношениях с Советом Европы «Завершение работ по модернизации Конвенции Совета Европы о защите данных (Конвенция 108) с целью присоединения ЕС к конвенции» и «Поддержка всемирной пропаганды этой Конвенции»[1].

В соответствии с таким развитием событий, позднее дополнение к проекту текста преамбулы к GDPR гласит, что, когда Комиссия при принятии решений об адекватности принимает во внимание международные обязательства третьей страны, «В частности, следует учитывать присоединение третьей страны к [Конвенции СЕ 108]» (пункт 81a). Это четкий сигнал всем неевропейским странам, заинтересованным в получении оценок адекватности ЕС, о том, что им следует рассмотреть предыдущую или одновременную заявку на присоединение к Конвенции 108.

Эти события в ЕС имеют значительные последствия как для глобализации, так и для модернизации Конвенции 108.

Директива 1995 года ознаменовала появление стандартов конфиденциальности данных «2-го поколения», которые в течение двух десятилетий имели большое влияние за пределами Европы, в той степени, в

[1] Council of the European Union, Political and Security committee – 1/A Item Note to Permanent Representatives Committee/Council ‘EU priorities for cooperation with the Council of Europe in 2016-2017’, Brussels, 15 December 2015, COSCE 7 CFSP/PESC 831 COHOM 121. ‘The Committee invites the Council, subject to approval by the Permanent Representatives, to adopt the priorities in the Annex’, one of which was Item 2.3 Rule of Law b. ‘Data protection’, as quoted above.

какой нынешний глобальный стандарт защиты конфиденциальности ближе к Директиве, чем к руководящим принципам ОЭСР[1].

Важным глобальным вопросом, касающимся GDPR, является вопрос о том, какие из его новых принципов содержания и требований к обеспечению соблюдения, вероятно, станут стандартными элементами законов о конфиденциальности данных за пределами ЕС: «3-е поколение» развивающихся глобальных стандартов конфиденциальности данных. В Европе это будет зависеть (но не полностью определено) от того, какие новые элементы GDPR станут, по существу, частью модернизированной Конвенции 108. За пределами Европы смесь влияния предполагаемых требований «адекватности» в GDPR, того, что требуется для присоединения к Конвенции 108, и желания подражать европейским «лучшим практикам» будет иметь влияние. И не следует забывать, что некоторые из «новых» элементов GDPR уже введены в действие за пределами ЕС (или включены в пересмотренные Руководящие принципы ОЭСР 2013 года) и поэтому по своей сути являются глобальными, а не европейскими.

Необходимо некоторое время, чтобы был виден результат, но список кандидатов на стандарты «3-го поколения» (после более детального рассмотрения) включает следующее:

1. Права распространяются на всех субъектов данных, независимо от национальности/места жительства;

2. Более строгие требования к согласию, включая ‘однозначные’ и разделяющие требования;

3. Право на переносимость пользовательского контента (UGC);

---

[1] For justification of this conclusion, see Greenleaf, G 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108' *International Data Privacy Law*, Vol. 2, Issue 2, 2012 < [Электронный ресурс] // http://ssrn.com/abstract=1960299>; and G Greenleaf Asian Data Privacy Laws (OUP, 2014), Chapter 17. (дата обращения: 10.06.2021).

4. Право на удаление/ ‘быть забытым»;

5. Обязательные сотрудники по защите данных (DPO) для конфиденциальной обработки;

6. Обязательные оценки воздействия на защиту данных (DPIAs) для обработки с высоким риском;

7. Защита данных по дизайну и по умолчанию;

8. Прямая ответственность как за процессоры, так и за контроллеры;

9. Иностранные контролеры должны быть представлены в пределах юрисдикции;

10. Уведомление о нарушении данных как DPA, так и в случае высокого риска для субъектов данных;

11. Групповые иски групп по защите частной жизни, представляющих общественный интерес;

12. Максимальные штрафы, основанные на мировом годовом обороте;

13. DPA должны принимать решения и применять административные санкции;

14. Право на судебное обжалование решений DPA;

15. DPA должны сотрудничать в разрешении жалоб с международными элементами;

16. От контролеров данных требуется наглядная подотчетность.

Все эти пункты содержатся в GDPR и/или проекте модернизированной Конвенции 108, а в нескольких случаях в пересмотренных Руководящих принципах ОЭСР 2013 года. Можно сказать, что некоторые из них подразумеваются Директивой 1995 года (возможно, включая 1, 7 и 9 выше), но теперь они стали более явными и важными для современного общества, которое претерпевает глобализацию, и поэтому включены в приведенный выше список. Оглядываясь назад, мы увидим, что не все из них будут частью новых глобальных стандартов (путем принятия национальных законов за пределами ЕС), но многие из них станут.

Закон о судебной защите США «уполномочивает Министерство юстиции (DOJ) назначать иностранные страны или региональные организации экономической интеграции, физические лица которых могут подавать гражданские иски в соответствии с Законом о конфиденциальности 1974 года против определенных государственных учреждений США в целях доступа, изменения или исправления незаконного раскрытия записей, переданных из иностранного государства в Соединенные Штаты, для предотвращения, расследования, выявления или судебного преследования за уголовные преступления»[1]. Эта часть пакета мер, направленных на решение проблем передачи персональных данных ЕС в США, обострилась из-за решения Шремса, принятого Палатой представителей в октябре. Судебный комитет Сената 28 января направил законопроект в полный состав Сената, но добавил дополнительные усложняющие условия. В упомянутом выше «боковом письме ТТП между США и Австралией» также предусматривается, что США «также будут стремиться распространить меры защиты конфиденциальности в отношении личной информации иностранных граждан, хранящейся правительством Соединенных Штатов, на граждан Австралии и постоянных жителей». Очевидно, Канада не добилась никаких таких уступок, поэтому не все стороны ТТП сделали это.

Нововведением явилось то, что 16 июля 2020 г. Суд Европейского союза (CJEU) прекратил передачу персональных данных с целью получения прибыли так называемым EU - US Privacy Shield. Данным путем шли многие американские компании, но теперь, например, Facebook не имеет права действовать по данным правилам и передавать данные пользователей в Евросоюз. Основной причиной такого запрета стала недостаточная степень

[1] Summary of House Bill 1428 [Электронный ресурс] // < https://www.congress.gov/bill/114th-congress/house-bill/1428 (дата обращения: 10.06.2021)

защиты данных граждан США от излишнего интереса со стороны органов государственной власти.

После GDPR наиболее важным фактором, влияющим на глобальное развитие стандартов конфиденциальности, остаются европейские (как ЕС, так и Совет Европы), небсмотря на то, что европейские юрисдикции в настоящее время составляют меньшинство тех, в которых действуют законы о конфиденциальности данных. Наиболее серьезный вызов этой правовой гегемонии по-прежнему исходит от Соединенных Штатов, как из-за их способности формировать Соглашения о свободной торговле, которые угрожают наложить ограничения на экспорт данных, так и из-за глобальной повсеместности и экономической мощи тех из их предприятий, которые основаны на использовании персональных данных. Как только у них возникает право передавать персональные данные в «безопасную гавань» США, они начинают действовать относительно безнаказанно по отношению к законам других стран. В эту игру играют уже почти 40 лет, и обе стороны снова обновляют свою тактику и проверяют, кто в их команде.

ЗАКЛЮЧЕНИЕ

Крупные социокультурные процессы глобализации и информатизации имеют качественное влияние на современные социальные, политические, экономические, правовые и иные институты. Развитие информационных технологий способствовало появлению информационного общества. В означенных условиях такой ресурс как информация получает новое значение. Таким образом, одной из центральных задач международного сообщества и национальных правопорядков стала защита национальных интересов в информационной сфере. О необходимости выработки в Российской Федерации универсального механизма защиты персональных данных свидетельствуют статистические данные: Positive Technologies провели исследование, согласно которому на Россию приходится около 10% всех совершенных в мире кибератак и киберпреступлений; по данным международного союза элекросвязи (специализированного учреждения ООН) Российская Федерация занимает пятое место в рейтинге кибербезопасности.

Нормативное правовое регулирование института персональных данный в Российской Федерации составляют Федеральный закон «О персональных данных», Федеральный закон «Об информации, информационных технологиях и о защите информации», а также иные федеральные законы, содержащие отдельные разъяснения по вопросам защиты персональных данных.

Анализ судебной практики, проведенный в настоящей работе, свидетельствует об отсутствии единообразного понимания правоприменителем способов, приемов, механизмов защиты персональных данных. Важный шаг в развитии отечественного законодательства сделал Конституционный Суд РФ, разграничив императивный запрет на поиск и распространение персональных данных без согласия лица и норму, допускающую свободное использование информации. Неоднозначно в судебной практике разрешается вопрос предоставления персональных данных

по запросу органов государственной власти. Хотя закон запрещает распространение персональных данных оператором и иными лицами, обладающими такой информацией (без согласия заинтересованного лица), суды часто встают на защиту государственных органов и их территориальных структур, запрашивавших подобные сведения.

В работе был исследован зарубежный опыт нормативного регулирования института персональных данных. Так, автором были изучены общие положения Директивы Европейского Парламента и Совета Европейского Союза 95/46/ЕС от 24 октября 1995 г. «о защите физических лиц при обработке персональных данных и о свободном обращении таких данных», Конвенции Совета Европы о защите данных, в частности «Конвенция о защите физических лиц при автоматизированной обработке персональных данных», руководящих принципов ОЭСР и рамках конфиденциальности АТЭС. Исходя из содержания указанных актов, можно сказать, что хотя все они призваны установить общие положения о защите персональных данных, в них отражены различные принципы охраны подобной информации. Таким образом, значение указанных декларативных актов видится в их взаимодополнении, связи друг с другом, что позволяет национальным правопорядкам устанавливать более специальные нормы о защите информации, содержащиеся, например, в федеральных законах. Проведенный анализ законодательных актов по защите персональных данных говорит нам о высокой значимости и необходимости решения данной проблемы не только для рядовых граждан, но и для государства в целом. Законы во многом похожи друг на друга и преследуют общую цель — гарантия защиты и юридическая поддержка граждан в решении проблем защиты конфиденциальных данных.

Проведенные автором исследования показали, что существуют различия в обеспечении защиты персональных данных в законодательных актах России и стран Европейского Союза. Так, в отечественном нормативном регулировании требования защиты персональных данных определяются

регулирующими органами, во многом не учитывается характер защищаемой информации, в то время как зарубежное законодательство демонстрирует гибкий подход к созданию систем защиты персональных данных.

Таким образом, законодательное регулирование и правоприменительная практика защиты персональных данных нуждаются в совершенствовании и дельнейшем развитии. Представляется, что перспективным способом такого развития является анализ зарубежного законодательного опыта защиты персональных данных. Разрешение сложившихся доктринальных и практических проблем, связанных с защитой персональных данных, станет возможным лишь при соответствующем уровне теоретической разработки института защиты персональных данных.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Нормативные правовые акты и документы стратегического планирования

1.1. Всеобщая декларация прав человека (Принята резолюцией 217 А (III) Генеральной Ассамблеи ООН от 10 декабря 1948 года) [Электронный ресурс] // Организация объединенных наций. – URL: https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml (дата обращения: 29.05.2021).

1.2. Конституция Российской Федерации (Принятая всенародным голосованием 12 декабря 1993 г.) // Собрание законодательства Российской Федерации. – 2014. – 31. – Ст. 4398.

1.3. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» // Собрание законодательства Российской Федерации. – 2003. – № 28. – Ст. 2895.

1.4. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» // Собрание законодательства Российской Федерации. – 2006. – № 31. – Ст. 3448.

1.5. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации. – 2006. – № 31 (1 ч.) – Ст. 3451.

1.6. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства Российской Федерации. – 2017. – № 31. – Ст. 4736.

1.7. Федеральный закон от 1 мая 2019 г. № 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации. – 2019. – № 18. – Ст. 2214.

1.8. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской

Федерации» // Собрание законодательства Российской Федерации. – 2016. – №50. – Ст. 7074.

1.9. Постановление Правительства Российской Федерации от 15 апреля 2014 г. № 313 «Об утверждении государственной программы Российской Федерации «Информационное общество» // Собрание законодательства Российской Федерации. – 2014. – № 18. – Ст. 2159.

1.10. Постановление Правительства РФ от 13 февраля 2019 г. N 136 «О Центре мониторинга и управления сетью связи общего пользования» // СПС «Консультант Плюс»

1.11. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года», утвержденные Президентом Российской Федерации 24 июля 2013 г. № Пр-1753. – Документ опубликован не был.

1.12. Паспорт национальной программы «Цифровая экономика Российской Федерации», утвержденный президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам, протокол от 24 декабря 2018 г. № 16. –Документ опубликован не был.

1.13. Закон КНР «О государственной безопасности» (утвержден 1 июля 2015 г. на заседании ПК ВСНП) [Электронный ресурс] // Chinalaw.center. – URL: https://chinalaw.center/administrative_law/china_state_security_law_2015_russian/ (дата обращения: 17.09.2020).

1.14. Закон КНР «О кибербезопасности» (утвержден в 7 ноября 2016 г. на заседании ПК ВСНП) [Электронный ресурс] // Cyberspace Administration of China. – URL: https://www.dezshira.com/library/legal/cyber-security-law-china-8013.html (дата обращения: 18.05.2021).

1.15. Национальная стратегия по безопасности в киберпространстве КНР (разработана Администрацией по делам киберпространства КНР в 2016 г.) [Электронный ресурс] // Cyberspace Administration of China. – URL:

http://www.cac.gov.cn/2016-12/27/c_1120195926.htm (дата обращения: 18.05.2021).

1.16. Определение Конституционного Суда РФ от 26.05.2016 N 1158-О «Об отказе в принятии к рассмотрению жалобы гражданки Сазоновой Елены Александровны на нарушение ее конституционных прав статьей 7 Федерального закона «О персональных данных» // СПС «Консультант Плюс»

1.17. International Strategy of Cooperation on Cyberspace (published by Ministry of Foreign Affairs and State Internet Information Office in 2017) [Электронный ресурс] // Xinhuanet. – URL: http://www.xinhuanet.com/english/china/2017-03/01/c_136094371.htm (дата обращения: 20.09.2021).

1.18. Regulations for safety protection of computer information systems (Promulgated by Decree № 147 of the State Council of the People's Republic of China in 1994) [Электронный ресурс] // AsianLII. – URL: http://www.asianlii.org/cn/legis/cen/laws/rfspocis719/ (дата обращения 17.09.2021).

1.19. Measures for security protection administration of the international networking of computer information networks (promulgated by Decree № 33 of the Ministry of Public Security in 1997 [Электронный ресурс] // AsianLII. – URL: http://www.asianlii.org/cn/legis/cen/laws/mfspaotinocin1194/ (дата обращения: 17.09.2021).

1.20. National cyber strategy of the United States of America (signed by the President of the United States of America in 2017) [Электронный ресурс] // White house. – URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (дата обращения: 22.04.2021).

1.21. Executive Order «Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities» [Электронный ресурс] // the White House President Barack Obama. – URL:

https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m (дата обращения: 24.05.2021).

1.22. Executive Order «Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities» [Электронный ресурс] // U.S. Department of States. – URL: https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber2_eo.pdf (дата обращения: 24.05.2021).

1.23. Digital Economy Act 2010 [Электронный ресурс] // legislation.gov.uk. – URL: https://www.legislation.gov.uk/ukpga/2010/24/contents (дата обращения: 25.05.2021).

1.24. National Cyber Security Strategy 2016 to 2021 [Электронный ресурс] // Gov.uk. – URL: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 (дата обращения: 25.05.2021).

1.25. Army Law of the Islamic Republic of Iran № 58 [Электронный ресурс] // Laws and regulation portal of Iran. – URL: http://law.dotic.ir/AIPLaw/lawview.do?reqCode=lawView&lawId=83349&type=all&isLaw=1 (дата обращения: 26.05.2021).

1.26. Resolutions of the Supreme Council on Cyberspace of Iran [Электронный ресурс] // Pars Times. – URL: http://majazi.ir/web_directory/web_directory/53298-عالی-شورای-مصوبات-فضای-مجازی.html (дата обращения: 25.07.2021).

2. Научная литература

2.1. Балашов А.Н. Правовое регулирование Интернет - отношений: основные проблемы и практика реализации в России [Электронный ресурс] // Cyberleninka. – URL: https://cyberleninka.ru/article/n/pravovoe-regulirovanie-internet-otnosheniy-osnovnye-problemy-i-praktika-realizatsii-v-rossii (дата обращения: 12.08.2021).

2.2. Винник Д. В. Цифровой суверенитет: политические и правовые режимы фильтрации данных [Электронный ресурс] // Издательство сибирского отделения Российской Академии Наук. – URL: http://sibran.ru/upload/iblock/f56/f56d5f4de7daf5c144d8597edf32e1eb.pdf (дата обращения: 02.05.2021).

2.3. Даниленков А. В. Государственный суверенитет Российской Федерации в информационно-телекоммуникационной сети «Интернет» [Электронный ресурс] // Cyberleninka. – URL: https://cyberleninka.ru/article/n/gosudarstvennyy-suverenitet-rossiyskoy-federatsii-v-informatsionno-telekommunikatsionnoy-seti-internet (дата обращения: 12.07.2021).

2.4. Ибрагимова Г. Стратегия КНР в области управления Интернетом и обеспечения информационной безопасности [Электронный ресурс] // ПИР- Центр.
URL: https://pircenter.org/media/content/files/10/13559074100.pdf (дата обращения: 17.05.2021).

2.5. Кучерявый М. М. К осознанию информационного суверенитета в тенденциях глобального информационного пространства [Электронный ресурс] // Научная электронная библиотека Elibrary.ru. – URL: https://elibrary.ru/item.asp?id=25846183 (дата обращения: 01.05.2021).

2.6. Разумов Е. А. Политика КНР по обеспечению кибербезопасности [Электронный ресурс] // Cyberleninka. – URL: https://cyberleninka.ru/article/n/politika-knr-po-obespecheniyu-kiberbezopasnosti (дата обращения: 17.08.2021).

2.7. Россошанский А. В. Политический и информационный суверенитет в контексте процессов глобализации пространства [Электронный ресурс] // Научная электронная библиотека Elibrary.ru. – URL: https://elibrary.ru/item.asp?id=17658015 (дата обращения: 01.05.2021).

2.8. Абрамова А. Г. Современные проблемы осуществления защиты персональных данных в сети: основополагающие принципы защиты персональных данных // Регион и мир. 2020. № 4. С. 21-25.

2.9. Максутов Б. М. Правовой механизм защиты персональных данных в Казахстане на основе общего регламента по защите персональных данных (GDPR) // INTERNATIONAL SCIENTIFIC REVIEW OF THE PROBLEMS OF LAW, SOCIOLOGY AND POLITICAL SCIENCE. 2019. С. 23-35.

2.10. Binxing F. Necessities for Advocating Cyberspace Sovereignty [Электронный ресурс] // Springer link. – URL: https://proxylibrary.hse.ru:2084/chapter/10.1007/978-981-13-0320-3_4 (дата обращения: 16.09.2021).

2.11. Li H. Regulation of Cyber Space: An Analysis of Chinese Law on Cyber Crime [Электронный ресурс] // International Journal of Cyber Criminology. – URL: https://www.cybercrimejournal.com/Li2015vol9issue2.pdf (дата обращения: 20.09.2021).

2.12. Liaropoulos A. N. Cyberspace governance and state sovereignty [Электронный ресурс] // Springer Link. URL: https://link.springer.com/chapter/10.1007/978-3-319-52168-8_2 (дата обращения: 08.09.2021).

2.13. Shaw S. R. There is no silver bullet: solutions to Internet jurisdiction // International Journal of Law and Information Technology. – 2017. – Т. 25. – № 4. – С. 283-308.

2.14. Summary of House Bill 1428 [Электронный ресурс] // < https://www.congress.gov/bill/114th-congress/house-bill/1428 (дата обращения: 10.06.2021)

3. Отчеты и информационные материалы

3.1. Дзядко Т., Канаев П., Девяткина М. Акимов объяснил неспособность Роскомнадзора заблокировать Telegram [Электронный ресурс] // РБК. –

URL: https://www.rbc.ru/technology_and_media/12/02/2019/5c62657d9a7947c3c09df809 (дата обращения: 09.10.2021).

3.2. Интернет в России: динамика проникновения. Зима 2017–2018 гг. [Электронный ресурс] // ФОМ. – URL: https://fom.ru/SMI-i-internet/13999 дата обращения: 13.10.2021).

3.3. Интернет в России: состояние, тенденции и перспективы развития. Аналитический отчет [Электронный ресурс] // РАЭК. – URL: https://raec.ru/activity/analytics/10122/ (дата обращения: 10.10.2021).

3.4. Ли И. Россия стала второй после США по количеству кибератак [Электронный ресурс] // РБК. – URL: https://www.rbc.ru/technology_and_media/13/06/2017/593a9a749a794766d6b11c54 (дата обращения: 30.04.2021).

3.5. Регулирование Интернета: Практические примеры из разных стран [Электронный ресурс] // Организация по безопасности и сотрудничеству в Европе. – URL: https://www.osce.org/ru/fom/96526?download=true (дата обращения: 22.05.2021).

3.6. Цензура (контроль) в Интернете. Опыт Китая [Электронный ресурс] // Tadviser. URL: http://www.tadviser.ru/index.php/Статья:Цензура_(контроль)_в_интернете._Опыт_Китая (дата обращения: 15.06.2021).

3.7. Baezner M., Robin P. Trend Analysis: Cyber Sovereignty and Data Sovereignty [Электронный ресурс] // CSS Cyber Defense Project. – URL: http://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/20180907_MB_TA_Cyber%20sovereignty_V2_rev.pdf (дата обращения: 02.07.2021).

3.8. China’s First Cyber Security Law [Электронный ресурс] // Institute for Defense Studies and Analyses. – URL: https://idsa.in/backgrounder/china-first-cyber-security-law_apsingh_231216 (дата обращения: 16.05.2021).

3.9. Cilluffo F., Fixler A. Evolving Menace Iran’s Use of Cyber-Enabled Economic Warfare [Электронный ресурс] // Foundation for Defense of Democracies. – URL: https://www.fdd.org/wp-

content/uploads/2018/11/REPORT_IranCEEW.pdf (дата обращения: 25.04.2021).

3.10. Global Cybersecurity Index [Электронный ресурс] // Committed to connecting the world. – URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf (дата обращения: 30.04.2019).

3.11. In Response To Protests, Iran Cuts Off Internet Access, Blocks Apps [Электронный ресурс] // npr. – URL: https://www.npr.org/2018/01/03/575252552/in-response-to-protests-iran-cuts-off-internet-access-blocks-apps (дата обращения: 26.05.2019).

3.12. Laws of the People’s Republic of China [Электронный ресурс] // AsianLII. – URL: http://www.asianlii.org/cn/legis/cen/laws/ (дата обращения: 17.03.2021).