Федеральное государственное автономное образовательное учреждение высшего образования
«Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)»

*На правах рукописи*

**Ван Гуанлун**

# ПУБЛИЧНО-ПРАВОВЫЕ МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В РОССИЙСКОЙ ФЕДЕРАЦИИ И КИТАЙСКОЙ НАРОДНОЙ РЕСПУБЛИКЕ: СРАВНИТЕЛЬНОЕ ИССЛЕДОВАНИЕ

5.1.2. Публично-правовые (государственно-правовые) науки

ДИССЕРТАЦИЯ
на соискание ученой степени кандидата юридических наук

Научный руководитель
доктор юридических наук, профессор
Минбалеев Алексей Владимирович

Москва - 2026

# ОГЛАВЛЕНИЕ

**ВВЕДЕНИЕ**..... 4

**ГЛАВА I. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**..... 24

1.1 Понятие персональных данных..... 24

1.2 Правовая природа персональных данных и их категорирование..... 31

1.3 Теоретические основы публично-правового обеспечения безопасности персональных данных граждан..... 37

**ГЛАВА II. ПУБЛИЧНО-ПРАВОВЫЕ МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В КИТАЕ И РОССИИ**.... 73

2.1 Конституционные основы обеспечения безопасности персональных данных граждан в Китае и России..... 73

2.2 Особенности административно-правового обеспечения безопасности персональных данных в Китае и России..... 90

2.3 Информационно-правовое обеспечение безопасности персональных данных в России..... 116

**ГЛАВА III. ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ПУБЛИЧНО-ПРАВОВОГО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В КИТАЕ И РОССИИ**..... 130

3.1 Формирование и развитие права на персональные данные в Китае и России как меры обеспечения безопасности персональных данных..... 130

3.2 Перспективы развития китайской и российской моделей публично-правового обеспечения безопасности персональных данных: сравнительный анализ..... 147

3.3 Основные направления совершенствования публично-правового обеспечения безопасности персональных данных в Китае и России..... 167

**ЗАКЛЮЧЕНИЕ** ..... 198

**СПИСОК СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ** ..... 208

**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ** ..... 210

**ПРИЛОЖЕНИЯ** ..... 235

# ВВЕДЕНИЕ

**Актуальность темы диссертационного исследования.** В условиях стремительного развития эры искусственного интеллекта и больших данных персональные данные граждан постоянно передаются в интерактивном режиме в Интернете, подвергаются огромному риску утечки. Данные – это новая движущая сила социального развития в условиях развития экономики данных, их ценность проистекает из их сущности, возможности их использования и иной обработки. Однако развитие современных информационно-телекоммуникационных технологий и многократное увеличение объемов обмена данными также привели к возникновению ряда рисков нарушения прав на личную информацию граждан. Персональные данные граждан в контексте больших данных представляют собой не только их основную персональную информацию, но и охватывают атрибуты идентичности человека и интересы граждан, которые проявляются в сочетании социально-экономической ценности с личными и общественными интересами. Нарушение прав на персональные данные затрагивает не только права и интересы отдельных граждан, но и интересы общества и государства.

Представляется, что стремительная цифровизация и детерминированная ею цифровая трансформация затронули все сферы жизни человека, оказав влияние на государство в политическом, культурном, экономическом, финансовом и социальном смыслах. Они оказали существенное влияние и на современное состояние персональных данных и осознание значимости обеспечения их безопасности, в том числе посредством применения публично-правовых мер. Причем характер угроз, связанных с обработкой персональных данных в современном мире, обусловливает приоритет публично-правовой защиты персональных данных.

В рамках научной работы был проведён опрос[1], направленный на изучение случаев утечки персональных данных студентов высших учебных заведений

[1] Анкета об утечке персональных данных на сайте Questionnaire Star (wjx.cn). URL: https://www.wjx.cn/xz/238487672.aspx (дата обращения: 21.02.2026).

Российской Федерации и Китайской Народной Республики (далее – России и Китая), [2] из которого можно сделать вывод, что утечка личной информации граждан приобретает устойчивую фиксируемую тенденцию. Подавляющее большинство утечек персональных данных относится к информации, которая тесно связана с личностью и имуществом отдельных граждан, а также с различными правонарушениями в цифровой среде. Формируется система способов и средств незаконного получения персональных данных, что наносит значительный ущерб как гражданам, так и обществу в целом. В условиях цифровой трансформации обработка и обеспечение безопасности персональных данных сталкиваются с серьезными рисками и вызовами.

Безусловно, большие данные, в том числе наборы персональных данных – это результат изменений, вызванных накоплением данных. Стремительное развитие машинного интеллекта привело к быстрому совершенствованию возможностей компьютерной обработки данных. В этой связи затраты на извлечение и обработку информации аналитиками из огромных массивов данных продолжают снижаться, а выгоды, получаемые от использования информации, многократно увеличиваются. В связи с этим персональные данные стали новым видом активов и объектом повышенной общественной значимости, а обеспечение их безопасности все более актуальным. Как государства с высоким уровнем развития цифровой среды, Китай и Россия должны глубоко осознавать необходимость создания эффективной системы обеспечения безопасности персональных данных.

Государство обязуется защищать основные права человека и гражданина. Права, связанные с информацией о личности, являются конституционной основой для защиты персональных данных граждан. Следовательно, обязанность государств по их защите является логической предпосылкой для публично-

[2] Для сбора данных использовалась функция создания и распространения анкет на платформе Questionnaire Star. После исключения недействительных ответов было получено 679 валидных анкет. Анализ достоверных данных показал, что 249 респондентов (36,67% от общего числа опрошенных) считают, что их личная информация была незаконно передана третьим лицам. Среди них: 70 анкет (28,11%) указывают на утечку данных вследствие использования деловых документов и различных квитанций; 57 анкет (22,89%) связаны с чрезмерным сбором персональных данных мобильными приложениями; 52 анкеты (20,88%) обусловлены утечкой информации из-за взлома учетных записей; 27 анкет (10,84%) связаны с утечкой данных через резюме; 21 анкета (8,43%) указывает на утечку информации при использовании общественного Wi-Fi; 22 анкеты (8,84%) описывают другие причины утечки персональных данных.

правового обеспечения безопасности персональных данных. Защита персональных данных регулируется законодательством, которое не только обеспечивает права граждан на конфиденциальность личной информации, но и тесно связано с вопросами национальной безопасности и защитой государственных интересов.[3] Помимо этого, оно значительно влияет на развитие свободной конкуренции, а также функционирование и развитие экономики данных. При этом нормативные правовые акты в различных государствах отличаются в зависимости от специфики защиты прав и интересов всех заинтересованных сторон. Это касается и законодательства о персональных данных в России и Китае.

Активное развитие процессов политического, экономического, социально-культурного и иных видов взаимодействия России и Китая требуют формирования эффективного информационного взаимодействия, в том числе посредством обеспечения безопасного оборота персональных данных как внутри государств, так и на уровне трансграничной передачи. В связи с этим важно исследовать и сопоставить ключевые особенности публично-правового обеспечения безопасности персональных данных в России и Китае, выявить необходимость их учета при совершенствовании законодательств обоих государств, а также обеспечения эффективной защиты права на персональные данные.

**Степень научной разработанности темы диссертационного исследования.** Вопросы правового регулирования персональных данных представляют собой предмет исследования ряда учёных-правоведов как в Китае, так и в России. Терминологический аппарат данного исследования был разработан на основе научных трудов в таких областях, как кибернетика, философия, история, социология и теория права.

Сложный и многоаспектный характер темы диссертации обусловил необходимость использования нескольких групп научных источников. К первой группе источников относятся научные труды ученых-юристов в области

[3] Ван Гуанлун. Механизм административного-правового регулирования защиты персональных данных в Китае: состояние, недостатки и путь решения. // Вестник Московского университета. 2024. Серия 11. Право. Том 65. № 4. С. 204-232.

информационного права и общей теории права о защите персональных данных: М.Ю. Авдеева, В.Н. Барсукова, И.Л. Бачило, Р.И. Бодрова, М.В. Бундина, М.А. Важоровой, Ван Лимина, Е.К. Волчинской, Гао Фупина, Э.М. Гатиятуллиной, Г.А. Грищенко, В.В. Гафнер, Дин Сяодуна, Р.И. Дремлюги, А.А. Ефремова, И.С. Иванова, В.П. Иванского, М.В. Кибакина, А.А. Кривоухова, Ли И, В.Н. Лопатина, А.В. Минбалеева, А.Г. Мираева, Т.А. Поляковой, А.И. Савельева, А.В. Серебренниковой, Л.К. Терещенко, М.А. Федотова, Фу Синьхуа, Цзян Юнфу, Цуй Гобина, Хэ Сюйсюя, Чэн Сяо, В.Н. Щепетильникова, Ян Фан и др.

Вторая группа состояла из научных работ, посвященных проблеме защиты персональных данных в контексте конституционного права, административного права и других отраслей права, - труды В.В. Архипова, И.В. Балашкиной, Ван Кая, И.А. Вельдера, М.В. Гализина, Гао Чжихуна, С.П. Гришаева, Н.Н. Далевской, Ду Цянцяна, Ду Чэнмина, М.О. Дьяконовой, А.А. Елисеевой, О.А. Зайцева, А.В. Кротова, Н.Е. Крыловой, Кун Фаньхуа, Б.М. Леонтьева, Ли Лея, А.М. Лушникова, Лю Гохуа, Ма Цзина, М.Н. Малеиной, И.Л. Петрухина, М.И. Проскуряковой, Пэн Чжуня, Пен Чуня, В.Д. Рузановой, Тан Жуйфан, Ю.С. Телиной, Д.Л. Ушкова, А.С. Федосина, Хан Даюаня, Э.А. Цадыковой, Цзи Яньминь, Чжан Вэйвэй, Чжан Вэньсяня, Чжао Чунли, Чжоу Вэйдуна, Чжоу Ханьхуа, Чэнь Танфы, И.А. Шевченко, Шен Вэйсина, Ян Ипина и др.

Работы данных авторов оказали существенное влияние на развитие исследования института персональных данных. Однако комплексный анализ данного института в контексте публично-правового обеспечения безопасности персональных данных и сравнительного анализа механизмов такой защиты в России и Китае остается недостаточно разработанным. В существующих научных трудах отмечается недостаток систематического изучения особенностей сочетания конституционно-правовых, административно-правовых и информационно-правовых механизмов обеспечения безопасности персональных данных. Кроме того, вопросы правовой защиты персональных данных в рамках китайского и российского конституционного, административного и информационного права требуют более глубокого и взаимосвязанного анализа. В связи с активным

развитием информационных технологий, укреплением связей с общественностью и совершенствованием законодательной базы в обоих государствах, актуальность данной проблемы продолжает оставаться высокой, а степень научной изученности явно недостаточной.

**Объектом диссертационного исследования** является совокупность общественных отношений, связанных с публично-правовым обеспечением безопасности персональных данных в современных правовых условиях в России и Китае.

**Предметом диссертационного исследования** выступает совокупность правовых норм, регулирующих вопросы обеспечения безопасности персональных данных в России и Китае, а также теоретические исследования и материалы судебной практики в данной сфере.

**Целью диссертационного исследования** является разработка и научное обоснование концептуальных основ правового института персональных данных с позиций сравнительного анализа публично-правовых мер обеспечения безопасности персональных данных в России и Китае, а также разработка предложений по совершенствованию данных мер и развитию соответствующего законодательства России и Китая.

Обозначенная цель предопределила решение следующих **задач исследования:**

— определить особенности понимания персональных данных в России и Китае;

— раскрыть правовую природу персональных данных и осуществить их категорирование;

— выявить теоретические основы публично-правового обеспечения безопасности персональных данных граждан;

— оценить конституционные основы обеспечения безопасности персональных данных в Китае и России;

— определить особенности административно-правового обеспечения безопасности персональных данных в Китае и России;

— выявить особенности информационно-правового обеспечения безопасности персональных данных в России;

— определить основные направления формирования и развития права на персональные данные в Китае и России как меры обеспечения безопасности персональных данных;

— исследовать перспективы развития китайской и российской моделей публично-правового обеспечения безопасности персональных данных на основе сравнительного анализа;

— выявить основные направления совершенствования публично-правового обеспечения безопасности персональных данных в Китае и России, а также разработать предложения по совершенствованию соответствующих механизмов.

**Методологическая основа диссертационного исследования** представляет собой совокупность используемых общенаучных методов познания (логический, диалектический, статистический, системный и др.), а также частноправовых методов (сравнительно-правовой, правового моделирования и др.).

Логический метод обеспечивает внутреннюю согласованность и непротиворечивость анализа, с его помощью были выстроены четкие дефиниции, проведены умозаключения о причинах сходств и различий в правовом регулировании и сформулированы аргументированные выводы и рекомендации. Диалектический метод позволяет рассматривать правовое регулирование и обеспечение безопасности персональных данных в России и в Китае как развивающийся процесс, внутренне полный противоречий. Системный метод использован для анализа публично-правовых механизмов обеспечения безопасности персональных данных в России и Китае как взаимосвязанных и внутренне организованных правовых комплексов. Он позволяет раскрыть специфику взаимодействия отраслевых мер, применяемых в целях защиты персональных данных. Статистический метод, в свою очередь, обеспечивает эмпирическую обоснованность исследования. Его применение связано с анализом данных о количестве и видах правонарушений в сфере персональных данных, а

также сведений о привлечении к административной ответственности в КНР и Российской Федерации. На этой основе оценивается эффективность правоприменительной практики, выявляются её основные тенденции и проблемные аспекты. Сравнительно-правовой метод выступает в качестве центрального инструмента исследования. Его применение позволяет провести детальное сопоставление правовых понятий, принципов, механизмов и процедур защиты персональных данных в законодательстве КНР и РФ, на основе этого сравнения выявляются как универсальные тенденции, так и уникальные для каждой правовой системы подходы, а также обнаруживаются правовые заимствования и расхождения. Метод правового моделирования позволяет выявить основные направления развития публично-правового обеспечения безопасности персональных данных и сформулировать модели совершенствования соответствующего регулирования в сфере персональных данных в России и Китае.

**Теоретическая основа** диссертационной работы представляет собой совокупность трудов российских ученых в области теории государства и права, информационного права, административного права, конституционного права, а также других отраслевых юридических наук, в частности: Бачило И.Л., Добробабы М.Б., Дремлюги Р.И., Иванова И.С., Иванского В.П., Кибакина М.В., Ковалевой Н.Н., Кривоухова А.А., Лескиной Э.И., Минбалеева А.В., Морозова А.В., Наумова В.Б., Поляковой Т.А., Савельева А.И., Смирнова А.А., Солдаткиной О.А., Сычева М. И., Чаннова С.Е., Чубуковой С.Г., Химченко А.И., Терещенко Л.К. и других; а также китайских исследователей: Ван Лимина, Гао Фупина, Дин Сяодуна, Ли И, Фу Синьхуа, Цзян Юнфу, Цуй Гобина, Хэ Сюйсюя, Чэн Сяо, Ян Фан, Ван Кая, Гао Чжихуна, Ду Цянцяна, Ду Чэнмина, Кун Фаньхуа, Ли Лея, Лю Гохуа, Ма Цзина, Пэн Чжуня, Пен Чуня, Хан Даюаня, Цзи Яньминь, Чжан Вэйвэй, Чжан Вэньсяня, Чжао Чунли, Чжоу Вэйдуна, Чжоу Ханьхуа, Чэнь Танфы, Шен Вэйсина, Ян Ипина и др.

**Нормативную основу диссертационного исследования** составляют международные правовые акты в сфере защиты персональных данных,

Конституция Российской Федерации и Конституция Китайской Народной Республики, административное законодательство, информационное законодательство, федеральные законы о персональных данных, а также подзаконные нормативные правовые акты национального и ведомственного уровней, регулирующие вопросы защиты персональных данных в России и Китае, и соответствующие нормы законодательства ряда зарубежных государств.

**Эмпирическая основа диссертационного исследования** включает в себя материалы правоприменительной и судебной практики Российской Федерации и Китайской Народной Республики, а также статистические данные, данные социологического опроса.

**Научная новизна диссертационного исследования** обусловлена исследованием персональных данных как самостоятельного социально-правового феномена, обладающего уникальной правовой природой, и требующего специального публично-правового обеспечения безопасности от современных вызовов и противоправных посягательств. В результате проведенного анализа теоретических и прикладных аспектов публично-правового регулирования в данной сфере были сформулированы и научно обоснованы меры развития публично-правового обеспечения безопасности персональных данных, адаптированные к особенностям правовых систем Китая и России. Выявлены системные связи между отраслевым законодательством в системе публично-правового обеспечения безопасности персональных данных, определен оптимальный баланс между публичными и частными интересами в процессе обеспечения безопасности персональных данных, а также предложены пути совершенствования публично-правовых мер обеспечения безопасности персональных данных в России и Китае.

Научная новизна также выражается в том, что на основе проведенного сравнительного анализа публично-правовых мер по обеспечению безопасности персональных данных в России и Китае разработаны модели дальнейшего совершенствования законодательства обоих государств, учитывающих как национальную специфику, так и общепризнанные международные стандарты в

области обеспечения безопасности и защиты персональных данных, что в совокупности вносит значительный вклад в развитие сравнительного правоведения и создает прочную теоретическую основу для дальнейшего совершенствования правового регулирования в данной области в России и Китае.

**На защиту выносятся следующие основные положения,** содержащие элементы научной новизны и являющиеся результатом диссертационного исследования:

1. С точки зрения правовой природы персональных данных в Китае и России выявлены как общие черты, так и существенные различия. Общим является признание особых свойств персональных данных, включая их чувствительность, конфиденциальность и социальную значимость, обусловленные разнообразием их содержания и форм выражения. Что касается различий, то в основе китайского подхода лежит критерий «идентифицируемости» (прямой или косвенной), который выступает центральным элементом в разграничении охраняемой информации и сферы её свободного использования. Российское законодательство, определяя персональные данные как «любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу», формально задает сопоставимый по охвату нормативный критерий, акцентируя связь информации с конкретным лицом. Ключевое различие заключается не в абсолютной «широте» определения, а в системообразующем значении, которое придается этому критерию в правоприменительной практике, а также в методах его интерпретации контрольно-надзорными и судебными органами. Таким образом, российский подход потенциально формирует более широкое концептуальное поле для отнесения информации к персональным данным, что создает дополнительные гарантии защиты прав личности, но одновременно может порождать большую степень неопределенности в правоприменении, например, при определении применимости требований по обеспечению безопасности к тем или иным данным, имеющим признаки персональных.

2. Предложен новый системный подход к категоризации персональных данных в Китайской Народной Республике, основанный на динамической,

контекстуально-зависимой оценке их чувствительности. Установлено, что степень чувствительности личной информации зависит не только от её внутренних характеристик, а также от специфики и условий конкретного сценария (цели) её использования и совершения иных действий. Основная цель обеспечения безопасности персональных данных заключается в гарантировании защищенности прав и законных интересов субъектов персональных данных, в минимизации рисков, связанных с их использованием и совершением иных действий с ними, в том числе на предотвращение возможных негативных последствий таких действий, а также восстановление нарушенных прав. Для адаптации к особенностям определения чувствительной личной информации, основанному на контексте конкретных сценариев (целей), рекомендуется внедрение разработанного системного подхода к обеспечению безопасности данных, подразумевающего внедрение публично-правовых мер, основанных на соответствующих правовых толкованиях, административных регламентах и отраслевых правилах. Выявлено, что такая динамическая дифференциация способствует повышению предсказуемости и эффективности обработки данных, оптимизации корпоративного комплаенса и связанных с ним затрат, что, в свою очередь, создает благоприятные условия для развития экономики данных.

Установлено, что подход к категорированию персональных данных, установленный в Российской Федерации, учитывая особенности обработки и защиты персональных данных, в целом отвечает требованиям публично-правового обеспечения их безопасности. В сравнительном аспекте отмечено, что выделение в Российской Федерации биометрических персональных данных в отдельную категорию, обособленную от специальных категорий персональных данных, создаёт дополнительные сложности в правоприменении и административные барьеры, не всегда соотносимые с гибкостью риск-ориентированного подхода.

3. Человеческое достоинство и свобода информации формируют фундаментальную ценностную основу правового, в том числе публично-правового, обеспечения безопасности персональных данных. Это проявляется в том, что, с одной стороны, личная информация является непосредственным

отражением достоинства и законных интересов субъекта информации, а с другой стороны, в соответствии с закрепленным в Китае принципом ценности свободы информации, обработка личной информации получает правовое обоснование. Показано, что такой ценностный дуализм находит конкретное выражение в законодательстве России и Китая, определяя различные подходы к построению баланса между обеспечением безопасности персональных данных и их обработкой.

При этом правовое обеспечение безопасности персональных данных должно в первую очередь основываться на содержании человеческого достоинства, что проявляется в признании за субъектом персональных данных комплекса правомочий по контролю над своей личной информацией. Однако право на защиту персональных данных не признается абсолютным и должно рассматриваться в соответствии с его социальной функцией. Это означает, что оно должно быть сбалансировано с другими основными правами и законными интересами в соответствии с принципом пропорциональности, что находит свое отражение в установлении законодательных ограничений и исключений из общего режима защиты.

Сравнительный анализ российского и китайского законодательства в данной сфере позволяет не только выявить различные акценты в решении проблемы баланса, но и определить взаимополезные элементы для совершенствования обеих систем с учётом их правовых традиций. Российский подход с его детализированной процедурной регламентацией оснований обработки данных может служить ориентиром для повышения формальной определённости и предсказуемости применения принципа соразмерности в китайском правоприменении. В свою очередь, китайский опыт чёткого нормативного закрепления приоритета публичных интересов (национальной безопасности, общественного благополучия) в определённых законом случаях предлагает модель для более структурированного и транспарентного учёта этих интересов в российской правовой системе, особенно в контексте регулирования новых технологий. Таким образом, потенциал для взаимного совершенствования лежит

не в заимствовании ценностных приоритетов, а в адаптации конкретных правовых механизмов и процедур: Россия может обогатиться более гибкими формулировками исключений в интересах общества, а Китай – более чёткими публично-правовыми мерами обеспечения безопасности в процессе обработки персональных данных и процессуальными гарантиями для защиты прав субъектов данных.

4. Установлено, что теоретической основой защиты персональных данных как в России, так и в Китае выступает механизм обеспечения баланса интересов. В Китае он концептуализирован в рамках «персональной кибернетики» и «социальной кибернетики», в России – в форме принципа баланса интересов личности, общества и государства, активно реализуемого в системе правового обеспечения информационной безопасности. Данный механизм направлен на определение, выявление и защиту прав и законных интересов граждан, связанных с персональными данными, с использованием комплекса правовых средств.

В целях повышения эффективности данного механизма представляется необходимым дальнейшее развитие и конкретизация системы действующих принципов правового регулирования персональных данных в обоих государствах через призму задачи обеспечения баланса. Такой подход подразумевает, что баланс интересов всех участников отношений в сфере персональных данных должен выступать не только как отдельный принцип, но и сквозной целью применения других существующих принципов, таких как законность, справедливость, соразмерность, целевое ограничение и минимизация данных и других. Это будет способствовать совершенствованию нормативных правовых актов, обеспечивая признание приоритета личностного достоинства, учёт общественных и государственных интересов, а также выявление и предотвращение потенциальных конфликтов между различными субъектами в процессе обеспечения безопасности и принятие мер защиты персональных данных.

Таким образом, научный и практический акцент смещается с провозглашения отдельного принципа баланса на анализ и оптимизацию взаимодействия

конкретных правовых принципов и механизмов, которые фактически уже опосредуют достижение этого баланса в национальных механизмах обеспечения безопасности персональных данных.

5. В рамках информационно-правового обеспечения безопасности персональных данных обоснованным представляется развитие концепции права на персональные данные как особого вида субъективных прав. При этом важно уточнить его соотношение с уже сформировавшимся в российской доктрине и практике понятием «права на защиту персональных данных», производного от права на неприкосновенность частной жизни. Предлагаемая конструкция «права на персональные данные» рассматривается не как альтернатива, а как следующая ступень развития субъективных прав в контексте цифровой трансформации, смещающая акцент с пассивной «защиты» на активное правомочие по распоряжению и контролю над своими данными в рамках, установленных законом. Ценность данного подхода заключается в создании более гибкого и технологически нейтрального концептуального инструмента для механизма обеспечения безопасности персональных данных.

Во-первых, хотя абсолютный индивидуальный контроль над информацией (информационное самоопределение) не всегда соответствует природе информационного обмена, признание за субъектом определённого объёма правомочий по контролю и участию в процессах обработки его данных является необходимым. Во-вторых, данная концепция отличается гибкостью, позволяющей учитывать динамику современного развития технологий и обеспечивать защиту достоинства личности в новых условиях цифровой среды.

При формировании китайской и российской моделей информационного права определение места этого права в системе правоотношений влияет на создание целостного механизма защиты. В контексте системы субъективных прав в информационной сфере предлагается рассматривать право на персональные данные как правомочие, производное не только от охраны человеческого достоинства, но и от совокупности конституционных ценностей: неприкосновенности частной жизни, личной и семейной тайны, права на

свободное развитие личности и защиты от произвольного вмешательства. Такой подход позволяет сбалансированно сочетать защиту прав субъектов данных с потребностями информационного общества, обеспечивая системное развитие информационного права.

6. Обосновано, что принципы обработки персональных данных выступают одной из базовых публично-правовых мер обеспечения безопасности персональных данных как в Российской Федерации, так и в Китайской Народной Республике. Они представляют собой совокупность идей, начал, универсально распространяемых на все отношения, складывающиеся в сфере обработки персональных данных, а также оказывающих непосредственное влияние на законодательство о персональных данных и правоприменительную практику в сфере обеспечения безопасности персональных данных. Установлено, что в качестве самостоятельного принципа обработки персональных данных необходимо рассматривать принцип обеспечения конфиденциальности персональных данных.

Данный принцип обеспечивает реализацию главной особенности персональных данных как вида информации ограниченного доступа – распространение на них режима конфиденциальности и необходимости его соблюдения, независимо от того, были ли они раскрыты субъектом персональных данных или нет. Он предполагает недопустимость утраты конфиденциальности персональных данных, влияет на развитие законодательства о персональных данных в части обеспечения их конфиденциальности, а также оказывает воздействие на правоприменение при разрешении конкретных споров в сфере персональных данных.

7. Обосновано, что в условиях стремительного развития цифровых технологий в Китае и России, увеличения количества утечек персональных данных необходимо развитие системы административно-правового и информационно-правового обеспечения безопасности персональных данных, включая следующие меры: конкретизацию иерархических взаимосвязей между нормативными правовыми актами при их применении; интеграцию ресурсов

сетевого контроля с внедрением современных технологий больших данных, включая разработку комплексной платформы для мониторинга обработки персональных данных и совершенствование механизма контроля и надзора в целях обеспечения безопасности персональных данных; совершенствование системы административной поддержки для защиты персональных данных, а также усиление развития судебной защиты прав на персональные данные в интересах субъектов персональных данных и общества. Обоснована необходимость развития законодательства об административных правонарушениях в части обновления и уточнения составов административных правонарушений, в том числе с позиции дифференциации правонарушений и ответственности в зависимости от оператора персональных данных.

В целях обеспечения безопасности персональных данных при открытии государственных данных обоснована необходимость развития следующих мер: меры по обеспечению соблюдения баланса общественных интересов и законных интересов физических лиц в области защиты персональных данных на основе принципа соразмерности; создание и улучшение системы правового регулирования обеспечения доступности и открытого использования государственных данных; создание механизма оценки рисков в сфере открытия государством данных с целью улучшения системы обработки органами исполнительной власти персональных данных.

8. Российский и китайский подходы к правовому регулированию персональных данных демонстрируют различные методологические парадигмы, сформированные национальными правовыми традициями. В России доминирует информационно-правовая модель, основу которой составляют акты информационного законодательства (Федеральный закон «О персональных данных» и другие нормативные правовые акты), направленные на обеспечение безопасности персональных данных. В Китае сохраняется приоритет административно-правового регулирования, интегрирующего защиту данных в систему государственного управления, с постепенным включением элементов формирующегося цифрового законодательства. Несмотря на разную отраслевую

доминанту, оба подхода носят межотраслевой характер: российская система реализуется через взаимодействие специальных информационно-правовых и конституционных, административных, уголовно-правовых, гражданско-правовых мер обеспечения безопасности персональных данных, в то время как китайская модель сочетает конституционные основы и административный контроль с развивающимися частноправовыми инструментами в цифровой сфере. Это отражает общую тенденцию к комплексному регулированию персональных данных в условиях цифровой трансформации.

Установлено, что академическая институционализация исследований в области публично-правовой защиты персональных данных обусловлена во многом тем, что в России информационное право консолидировалось как комплексная отрасль права и самостоятельная отрасль юридической науки с оформлением отдельного предметного поля, созданием профильных кафедр и образовательных программ в ведущих юридических вузах. В Китае, несмотря на официальный статус в системе юридических дисциплин, «информационное право» развивается преимущественно в междисциплинарном режиме в рамках традиционных кафедр, что указывает на продолжающийся процесс его научно-образовательной институционализации как самостоятельной юридической науки и учебной дисциплины. Эти различия иллюстрируют более широкие дивергентные траектории адаптации разных правовых механизмов обеспечения безопасности персональных данных к вызовам цифровой трансформации. Данное различие обусловлено как особенностями правовых традиций двух государств, так и определёнными отличиями стратегических приоритетов развития в России и Китае. При том выявлено, что правовые системы России и Китая в части публично-правового обеспечения безопасности персональных данных демонстрируют тенденцию к конвергенции, адаптируясь к вызовам цифровой трансформации посредством развития межотраслевых механизмов правового регулирования персональных данных и публично-правового обеспечения их безопасности.

9. При сопоставлении институциональных моделей публично-правового

обеспечения безопасности персональных данных в Китае и России выявлены различные системные подходы, детерминированные национальными административными и правовыми традициями. Китайская модель характеризуется сетевым (полицентричным) регулированием с распределением компетенций между Центральным комитетом по вопросам киберпространства, Министерством промышленности и информатизации и Министерством общественной безопасности. Российская модель, напротив, воплощает функционально-концентрированную парадигму, где ключевые полномочия закреплены за Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации, Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), Федеральной службой безопасности Российской Федерации (ФСБ России) – в части установления требований к защите информации в государственных информационных системах и использования средств криптографической защиты и Федеральной службы по техническому и экспортному контролю (ФСТЭК России) – в части установления требований по защите информации ограниченного доступа от несанкционированного доступа.

**Теоретическая значимость диссертационного исследования** проявляется в углублении и систематизации научных представлений о публично-правовом обеспечении безопасности персональных данных в России и Китае, а также их развитии в условиях современных вызовов и угроз. Полученные результаты могут быть использованы в качестве фундаментальной основы для проведения последующих научных исследований, направленных на совершенствование публично-правового обеспечения безопасности персональных данных в России и Китае.

**Практическая значимость диссертационного исследования** проявляется в формулировании научно обоснованных моделей по дальнейшему совершенствованию публично-правового обеспечения безопасности персональных данных в России и Китае с учетом заимствования наиболее успешных механизмов. Полученные данные могут быть использованы и в

правоприменительной практике в сфере защиты персональных данных в России и Китае. Полученные результаты могут быть использованы для совершенствования нормативных правовых актов, подготовки аналитических обзоров судебной практики по вопросам правовой охраны персональных данных. Кроме того, материалы диссертационного исследования представляют ценность для интеграции в учебный процесс образовательных организаций высшего образования с целью совершенствования программ курсов публично-правовых наук.

**Соответствие диссертационного исследования паспорту научной специальности.** Работа соответствует пунктам 25 (Публично-правовое регулирование в сфере и информационных (цифровых) технологий, архивного дела и защиты информации) и 26 (Правовое регулирование использования информационных (цифровых) технологий при осуществлении публичной власти и в публичном управлении) паспорта научной специальности 5.1.2. Публично-правовые (государственно-правовые) науки.

**Степень обоснованности и достоверности диссертационного исследования и результатов исследования** обеспечивается применением широкого спектра общенаучных и частнонаучных методов познания, составляющих методологическую основу диссертационного исследования. В процессе работы были проанализированы значительные объемы данных, полученных ведущими учеными-правоведами в ходе многолетних исследований в области конституционного, административного и информационного права. Исследование опирается на информационно-справочные и документальные источники, материалы средств массовой информации, а также данные, размещенные в информационно-телекоммуникационной сети Интернет. Проведен сравнительно-правовой анализ обширной нормативной правовой базы, охватывающей как китайское и российское законодательство, так и зарубежное право, а также международные нормы, регламентирующие правовую защиту персональных данных. Особое внимание уделено анализу судебной и иной правоприменительной практики, связанной с привлечением лиц к

административной ответственности за нарушения в сфере персональных данных[4].

**Апробация результатов диссертационного исследования.** Диссертационная работа обсуждена на кафедре информационного права и цифровых технологий Московского государственного юридического университета имени О.Е. Кутафина (МГЮА) и рекомендована ею к защите. Отдельные положения и результаты диссертации нашли отражение в одной монографии и в 10 научных статьях, из которых 6 опубликованы в рецензируемых научных журналах, рекомендованных Высшей аттестационной комиссией при Министерстве науки и высшего образования РФ.

Теоретические положения, выводы и результаты исследования обсуждены и одобрены на заседании кафедры информационного права и цифровых технологий ФГАОУ ВО «Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)», а также прошли апробацию на международных научных и научно-практических конференциях и иных мероприятиях: Всероссийский круглый стол с международным участием на тему: «Место информационного права в публично-правовых (государственно правовых) науках» (Москв, 1 ноября 2023 г.), XXVI Международная научно-практическая конференция «Кутафинские чтения» (Москва, 26-29 ноября 2024 г.), Всероссийская научно-практическая конференция с международным участием «Использование современных цифровых технологий в правоохранительной деятельности» (20 сентября 2024 г.), II Международная научно-практическая конференция «Современное право КНР» (Санкт-Петербург, 18-19 апреля 2024 г.) Седьмая Международная научно-практическая конференция «Бачиловские чтения» (Москва, 6-7 февраля 2024 г.) II Международный форум китайско-российского сравнительного правоведения (КНР, Кайфэн, 6 апреля 2024 г.), Первый Российско-китайский Юридический Форум (МГЮА) (Москва, 28 ноября 2024 г.), Восьмая международная научно-практическая конференция по информационному праву и правовому обеспечению информационной безопасности «Бачиловские чтения» (Москва, 31 января 2025 г.),

[4] Ван Гуанлун. Административно-правовая защита персональной информации в Китае: недостатки и путь решения // Вестник Университета имени О.Е. Кутафина (МГЮА). 2024. № 10. С. 189-197.

IV Международная научно-практическая конференция «Цифровые технологии и право» (Казань, 19 сентября 2025 г.), XI Международная научно-практическая конференция «Российская правовая система и юриспруденция» (КНР, Шанхай, 11 октября 2025 г.), 4.0 Международная научно-практическая конференция «Цифровая трансформация: вызовы для права, образования и кибербезопасности» (Махачкала, 8 ноября 2025 г.).

**Структура и объем диссертационного исследования** определены исходя из его целей, задач и проблематики. Работа состоит из введения, трех глав, объединяющих девять параграфов, заключения и списка используемых источников.

# ГЛАВА I. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

## 1.1 Понятие персональных данных

Современные информационные технологии значительно трансформировали наше понимание конфиденциальности и личного пространства. Многие процессы, ранее происходившие в офлайн-среде, были подвергнуты цифровизации: электронная коммерция, онлайн-коммуникации с социальным окружением, взаимодействие с работодателями и государственными учреждениями. В результате объем персональных данных, раскрываемых пользователями в сети Интернет, а также собираемых и систематизируемых организациями различных типов, достиг беспрецедентных масштабов.[5]

Персональные данные – это сложный и формирующийся правовой феномен[6]. В связи с положениями закона перечень сведений, определяющих физических лиц, неуклонно расширяется, что усложнило взаимоотношения между субъектами правоотношений, возникающих по поводу персональных данных[7]. Несмотря на определенные преимущества расширения обмена информацией, возникают некоторые факторы, указывающие на то, что конституционные права граждан на неприкосновенность частной жизни, личную и семейную тайну находятся под

---

[5] *Савельев А.И.* Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) // Право. Журнал Высшей школы экономики. 2015. №1. С. 44.

[6] См.: *Полякова Т.А., Смирнов А.А.* Противодействие киберпреступности в новой цифровой реальности: вызовы и правовые решения // Государство и право. 2026. №. 2. С. 236-246; *Полякова Т.А., Смирнов А.А.* Правовые аспекты обеспечения информационной безопасности при использовании технологий искусственного интеллекта // Вестник Московского университета. Серия 26: Государственный аудит. 2024. № 3. С. 89-106; *Лескина Э.И.* Понятие и объект оборота данных // Законодательство. 2025. № 3. С. 42 49; *Лескина Э.И., Солдаткина О.Л.* Правовое регулирование оборота данных в цифровом виде в Индии: изменения последних лет и тенденции развития // Закон. 2025. № 8. С. 66-76; *Ковалева Н. Н., Жирнова Н. А.* Правовой режим персональных данных в социальных сетях: проблемы квалификации и практические аспекты обработки // Закон. 2025. № 9. С. 61–68; *Грищенко Г.А.* О некоторых актуальных проблемах защиты персональных данных граждан в цифровом пространстве // Аграрное и земельное право. 2025. № 9. С. 143-146; *Терещенко Л. К.* Государственный контроль в сфере за щиты персональных данных // Право. Журнал Высшей школы экономики. 2018. № 4. С. 142-161; *Морозов А.В., Филатова Л.В., Полякова Т.А.* Информационное право и информационная безопасность. Часть 2. Учебник. М.: РПА, 2016. 604 с.; *Морозов А.В., Филатова Л.В.* Правовые вопросы доступа к информации. Учебное пособие. М.: РПА, 2015. 82 с.; *Волчинская Е.К.* Защита персональных данных. Опыт правового регулирования. М.: Галерея, 2001. 236 с.; *Волчинская Е.К.* Место персональных данных в системе информации ограниченного доступа // Право. Журнал Высшей школы экономики.2014. № 4. 193-207.

[7] Право персональных данных : учебник / под ред. д-ра юрид. наук, профессора А. В. Минбалеева. 2-е изд., доп. и перераб. М.: Издательский центр Университета имени О.Е. Кутафина (МГЮА), 2025. С. 45.

угрозой[8]. Чтобы минимизировать эти угрозы важно решить проблемы, связанные с обработкой и защитой персональных данных. Прежде всего, необходимо определить содержание определения «персональные данные».

Персональные данные являются не только важным компонентом информационных ресурсов цифрового общества, но и предметом публично-правовой защиты. С развитием информационных технологий персональные данные становятся особым способом личного существования, особой формой идентичности личности.

Согласно законодательству о защите персональных данных, разработанному в различных государствах и регионах мира, терминология в этой области варьируется в зависимости от особенностей соответствующих правовых систем. Наиболее распространёнными понятиями являются «персональные данные», «персональная информация» и «право на неприкосновенность частной жизни»[9]. Например, концепция «права на неприкосновенность частной жизни» закреплена в законодательстве США[10]; термин «персональные данные» используется в нормативных актах Европейского союза[11] и ряда европейских государств и других государств мира[12]; понятие «персональная информация» применяется в Японском Законе о защите персональной информации (2003)[13] и Законе КНР о защите персональной информации (2021)[14].

По своему семантическому значению термины «персональные данные» и

---

[8] См.: *Симонова Е.В.* Определение понятия персональных данных в Российской Федерации // Молодой ученый. 2017. № 10 (144). С. 323.

[9] См.: *Чэн Сяо.* О правах на персональные данные в эпоху больших данных // Китайские общественные науки. 2018. № 03. С. 102-122.

[10] Здесь касается Закона США «О семейных и образовательных правах и неприкосновенности частной жизни» (1974). См.: Законодательства США в сфере защиты персональных данных. URL: https://4people.grfc.ru/analytics-and-legislation/international-and-foreign-acts/foreign-acts/ssha/ (дата обращения: 06.09.2024).

[11] Например, «Конвенция о защите физических лиц при автоматизированной обработке персональных данных» (1981 г.). URL: https://normativ.kontur.ru/document?moduleId=1&documentId=269845 (дата обращения: 06.09.2024); Директив ЕС о защите данных 95/46/ЕС (1995). URL: https://www.tgl.net.ru/files/infosafety/директива%2095-46.pdf (дата обращения: 06.09.2024).

[12] Например, Федеральный закон Германии о защите персональных данных (1977). См.: *Параскевов А.В., Левченко А.В., Кухоль Ю.А.* Сравнительный анализ правового регулирования защиты персональных данных в России и за рубежом // Научный журнал КубГАУ. 2015. № 110 (06). С. 878.

[13] Закон Японии о защите персональной информации (2003). URL: https://laws.e-gov.go.jp/law/415AC0000000057 (да та обращения: 06.09.2024).

[14] Закон КНР о защите персональной информации (2021). URL: http://www.npc.gov.cn/npc/c2/c30834/202108/t20210820_313088.html (дата обращения: 06.09.2024).

«персональная информация» обладают значительным сходством в контексте объектов исследования и содержания. В большинстве случаев различия между ними носят второстепенный характер и не оказывают существенного влияния на их применение.[15] Однако два вышеприведенных понятия и понятие «частная жизнь» пересекаются и исключают полное значимое совпадение, поэтому их нельзя интерпретировать как синонимы. В связи с этим, помимо понятия «частная жизнь», различия между понятиями «персональные данные» и «персональная информация», которые фигурируют в настоящей диссертации, не проводятся.

Как в законодательстве Европейского союза[16], так и в законодательстве США[17] существуют свои собственные уникальные определения понятия «персональные данные»[18].

В России некоторые аспекты права на неприкосновенность частной жизни были законодательно установлены и детально проанализированы ещё в дореволюционный период[19]: первые нормы защиты персональных данных

---

[15] См.: *Ван Чен.* Выбор модели гражданско-правовой защиты персональных данных // Китайские общественные науки. 2019. № 6. С. 124-146.

[16] Согласно Регламенту Европейского Парламента и Совета Европейского Союза 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных / General Data Protection Regulation /GDPR) персональные данные это любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу URL: https://base.garant.ru/71936226/1b93c134b90c6071b4dc3f495464b753/ (дата обращения: 02.09.2025).

[17] Закон США о неприкосновенности частной жизни 1974 года включен в главу V Федерального кодекса США. Согласно статье 552a, личная информация называется личной записью. Здесь термин «запись» означает «любой элемент, коллекцию или группировку информации о физическом лице, которая хранится агентством, включая, но не ограничиваясь, его образование, финансовые операции, историю болезни, криминальную или трудовую историю, а также его имя или идентификационный номер, символ или другую идентифицирующую деталь, присвоенную физическому лицу, такую как отпечаток пальца или голоса или фотография». Принятый в 2018 году Калифорнийский закон о защите конфиденциальности потребителей (California Consumer Privacy Act) стал знаковым законодательным актом в США, который позволил решить часть проблем, связанных защитой персональных данных, и создать прецедент для других штатов. См.: Закон США о неприкосновенности частной жизни 1974 года. https://www.archives.gov/about/laws/privacy-act-1974.html (дата обращения: 07.09.2024); *Рачицкая В.А.* К анализу современных тенденций в сфере защиты данных потребителей // Via scientiarum – Дорога знаний. 2019. № 4. С. 28-31.

[18] Современное американское законодательство, по сравнению с европейской моделью защиты персональных данных и Общим регламентом Европейского союза по защите персональных данных (GDPR), обладает собственными особенностями характерными для американской модели, а именно: секторальный и дифференцированный предмет регулирования отношений, большая направленность на обеспечение оборотоспособности персональных данных, создание эффективной системы защиты прав субъектами в судебном порядке (в том числе введение статутных убытков, которые являются, по своей сути, штрафами за нарушение прав субъектов персональных данных) и т.д. См.: *Писарев В.В.* Обзор развития законодательства США о персональных данных // Вопросы российского и международного права. 2023. Том 13. № 7А. С. 100.

[19] Например, Почтовый устав 1857 г. и Телеграфный устав 1876 г. закрепляли тайну корреспонденции, уголовно-правовая охрана указанной тайны осуществлялась на основании норм Уложения о наказаниях уголовных и исправительных 1845 г., Уголовного Уложения 1903 г. См.: Балашкина И.В. Особенности конституционного

рассматривались в рамках права на неприкосновенность частной жизни.

С развитием цифрового общества, характеризующегося широким внедрением информационных технологий и интенсивным сбором данных, включая персональные данные, возникла необходимость принятия специального законодательства для регулирования обработки таких данных.[20] В рамках данного процесса в 2006 году был принят Федеральный закон № 152-ФЗ «О персональных данных» (далее – ФЗ о ПДн)[21], который устанавливает правовые основы для регулирования отношений, связанных с автоматизированной обработкой персональных данных. В соответствии с пунктом 1 ст. 3 этого закона персональные данные определяются как «любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)»[22].

Согласно действующему законодательству Российской Федерации, персональные данные могут быть представлены в любой форме и включать различные категории информации, такие как: имя, адрес, контактные данные, фотографии, биометрические данные, медицинская информация, финансовая информация и любая другая информация, относящаяся к субъектам персональных данных[23]. При этом закон подчеркивает, что информация, не связанная с конкретным человеком, не может быть отнесена к категории персональных данных. Таким образом, определение персональных данных в российском законодательстве имеет значительное сходство с аналогичным определением в европейском законодательстве[24]. При этом важно отметить, что Федеральный закон от 30.12.2020 № 519-ФЗ «О внесении изменений в Федеральный закон «О

---

регулирования права на неприкосновенность частной жизни в Российской Федерации // Право и политика. 2007. №7. С. 95.

[20] См.: *Гуде С.В.* Защита персональных данных в Российской Федерации: исторический аспект и современное состояние // Юристъ-Правоведъ. 2015. № 2 (69). С. 95.

[21] О персональных данных: Федеральный закон от 27 июля 2006 года № 152-ФЗ: принят Гос. Думой 8 июля 2006 г.: одобрен Советом Федерации 14 июля 2006 г. // Российская газета. 2006. 29 июля.

[22] Там же.

[23] См.: *Гатиятуллина Э.М.* Защита персональных данных в условиях цифровизации: эволюция и современное состояние // Закон и власть. 2023. № 3. С. 33-37.

[24] Данное определение корреспондирует дефиниции, изложенной в Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных. См.: Право персональных данных: учебник / под об. ред. д.ю.н., профессора *А.В. Минбалеева.* – Саратов: ООО «Амирит», 2023. С. 46; *Мираев А.Г.* Понятие персональных данных в Российской Федерации и Европейском союзе // Юридическая наука. 2019. № 5. С. 76-82.

персональных данных» ввел новый правовой режим именно для персональных данных, разрешенных субъектом персональных данных для распространения[25].

В российской правовой доктрине и правоприменительной практике понятие персональных данных носит преимущественно прикладной, а не формально-описательный характер. В соответствии со статьей 3 Федерального закона «О персональных данных» персональные данные определяются как любая информация, относящаяся прямо или косвенно к определённому либо определяемому физическому лицу, что сознательно формулируется законодателем в максимально широкой и абстрактной форме . Как отмечает А. В. Минбалеев, ключевым признаком персональных данных является не вид или источник информации, а наличие фактической либо потенциальной возможности идентификации субъекта, вследствие чего правовая квалификация данных неизбежно зависит от конкретного контекста их обработки[26]. Анализ судебной практики, проведённый М. Б. Добробабой, демонстрирует, что такие сведения, как IP-адрес, номер телефона, адрес электронной почты, ИНН или паспортные реквизиты, признаются персональными данными не всегда, а лишь при условии их обработки в совокупности с иными сведениями, позволяющими определить субъекта персональных данных по ним, при этом подходы судов и надзорных органов остаются неоднородными [27] . Применительно ко многим данным необходимо в каждом индивидуальном случае смотреть позволяют ли отдельные данные определить субъекта или нет[28]. Очень часто о персональных данных

---

[25] *Минбалеев А.В.* Проблемы правового обеспечения кибербезопасности при распространении персональных данных в сети интернет по обновленному законодательству // Вестник УрФО № 2(40). 2021. С. 66.

[26] *Минбалеев А.В.* Проблемные вопросы понятия и сущности персональных данных // Вестник УрФО. Безопасность в информационной сфере. 2012. № 2 (14). С. 4-9.

[27] *Добробаба М.Б.* Понятие персональных данных: проблема правовой определенности // Вестник Университета имени О.Е. Кутафина (МГЮА). 2023. № 2(102). С. 42-52.

[28] См., например позицию судов: Решение Арбитражного суда г. Москвы от 10.12.2025 по делу № А40-201075/25 // СПС «Гарант»; Постановление Девятого арбитражного апелляционного суда от 14 апреля 2026 г. N 09АП-68401/25 по делу № А40-201075/2025 // СПС «Гарант»; Определение Верховного Суда РФ от 08.09.2020 № 308-ЭС20-11154 по делу № А63-13382/2019 // СПС «Гарант»; Постановление Второго арбитражного апелляционного суда от 08.08.2019 № 02АП-5517/2019 по делу № А31-3955/2019 // СПС «Гарант»; Определение Московского городского суда от 13.05.2019 № 4г-4164/19 // СПС «Гарант»; Решение Октябрьского районного суда г. Белгорода от 12 сентября 2019 г. по делу № 12-393/2019 // СПС «Гарант»; Постановление Седьмого арбитражного апелляционного суда от 05.04.2018 N 07АП-1437/2018 по делу № А45-31682/2017 // СПС «Гарант»; Определение Судебной коллегии по гражданским делам Верховного Суда РФ от 01.08.2017 № 78-КГ17-45 // СПС «Гарант»; Постановление Восемнадцатого арбитражного апелляционного суда от 05.04.2017 № 18АП-2210/2017 по делу № А07-24090/2016 // СПС «Гарант»; Апелляционное определение Санкт-Петербургского городского суда от 03.02.2015 № 33- 1644/2015 по делу № 2-3097/2014 // СПС «Гарант».

приходится говорить именно как о совокупности данных, которые и позволяют провести определение лица. Например, только по номеру ИНН или номеру телефона мы не сможем определить субъекта, но если к этим данным добавить фамилию имя и отчество их обладателя, то определение может быть произведено успешно. В этом случае мы и говорим о персональных данных. Следовательно, на практике персональные данные в российском праве представляют собой динамическую категорию, формируемую через критерий определяемости и уточняемую индивидуально к каждому конкретному случаю, в том числе часто в процессе правоприменения, а не исчерпывающий перечень информации, заранее заданный законом.

Что касается определения понятия персональной информации в Китае, то профессор Ван Лимин определяет «персональную информацию» как идентифицируемую символическую систему, отражающую индивидуальные характеристики, связанные с конкретным лицом[29]. По мнению профессора Чжоу Ханьхуа, ученого Китайской академии общественных наук, персональной информацией признается такая информация, которая может индивидуально или путем сравнения с другой информацией идентифицировать конкретного лица, включая личное имя, адрес, дату рождения, номер удостоверения личности, медицинские записи, записи в личном деле, фотографии и т.д.[30]. Среди китайских юристов выделялись и другие концепции, касающиеся определения личной информации[31]. Кроме того, в Гражданском кодексе КНР (далее – ГК КНР), опубликованном в 2020 году, также закреплено понятие персональной информации[32].

---

[29] *Ван Лимин.* Законы о правах личности. Пекин: Издательство Китайского народного университета. 2005. С. 633.

[30] См.: *Чжоу Ханьхуа.* Закон Китайской Народной Республики о защите персональной информации (проект рекомендаций экспертов) и отчет об исследовании законодательства. Пекин: Юридическая пресса. 2006. С. 3.

[31] Персональная информация определялась как «доступные ресурсы, такие как данные о личных характеристиках, данные и записи, которые выполняют функции социального взаимодействия, государственного управления и экономического развития» либо «частная информация, которая может идентифицировать конкретное физическое лицо и не имеет прямого отношения к общественным интересам». См.: *Гао Фупин.* Основа легитимности использования персональной информации: анализ выгод на данные // Журнал сравнительного правоведения. 2019. № 2. С. 72-85; *Лю Дэлян.* Защита прав собственности на персональную информацию // Китайский юридический журнал. 2007. № 3. С. 80-91.

[32] Согласно ст. 1034 ГК КНР 2020 года персональная информация означает информацию, записанную в электронном виде или другими способами, которая может использоваться сама по себе или в сочетании с другой информацией для идентификации физического лица, включая имя, дату рождения, номер удостоверения личности,

В 2021 году был принят специальный Закон КНР о защите персональной информации [33] (далее – Закон КНР о ПДн). Согласно статье 4 этого закона, персональной информацией являются **все виды информации,** записанные с помощью электронных или иных средств, **относящейся к идентифицированному или идентифицируемому физическому лицу**, за исключением информации после применения технологий анонимизации[34].

По сравнению с ГК КНР, Закон КНР о ПДн исключает выражение «… использоваться сама по себе или в сочетании с другой информацией» в целях расширения сферы защиты. Также важно отметить, что в Законе КНР о ПДн прямо предусмотрено, что информация после анонимизации не включается в понятие персональной информации, чтобы ограничить сферу правоприменения.

Таким образом, в вышеуказанных научных исследованиях и положениях законодательства, касающихся дефиниции «персональные данные», большинство государств пришли к единой позиции относительно «идентификации» («определения») личной информации. С развитием цифрового общества и постоянным обогащением и усложнением социальной деятельности человека увеличивается и содержание персональных данных. Более того, благодаря развитию науки и техники, большинство государств осознали, что биологическая информация о человеке является уникальной и эксклюзивной для определенного человека. Следовательно, постоянное обогащение содержания и объем личной информации заставляют государства по всему миру все шире определять понятие персональных данных.

Следует отметить, что в настоящей диссертации рассматриваются теории и правовые системы многих государств в области защиты персональных данных, а

---

биометрическую информацию, адрес проживания, телефонный номер, адрес электронной почты, информацию о здоровье, местоположение и иное. См.: Гражданский кодекс Китайской Народной Республики, принятый на третьей сессии 13-го Всекитайского собрания народных представителей 28 мая 2020 года. URL: http://www.npc.gov.cn/c2/c30834/202006/t20200602_306457.html (дата обращения: 07.09.2024).

[33] Некоторые китайские юристы переводят данный закон как не о персональной информации, а как о персональных данных. См.: Избранные нормативно-правовые акты Китайской Народной Республики в области цифровизации / пер. с кит Ли Яо. М.: Проспект, 2025. С. 37. Однако лингвистический анализ позволяет говорить, что более правильный перевод в данном случае именно персональная информация, а не персональные данные.

[34] Закон Китайской Народной Республики о защите персональной информации, принятый на 30-м заседании Постоянного комитета 13-го Всекитайского собрания народных Представителей Китайской Народной Республики 20 августа 2021 года и вступивший в силу 1 ноября 2021 года. URL: https://baijiahao.baidu.com/s?id=1708834553322434665&wfr=spider&for=pc (дата обращения: 07.09.2024).

термин, используемый в разных государствах для описания личной информации, имеет свою собственную концепцию[35].

При обсуждении соответствующих теорий и законов разных государств и регионов произвольное использование «персональных данных» вместо других терминов неизбежно приведет к различным толкованиям и проблемам в правоприменении. Поэтому в настоящей диссертации полагаем необходимым указать, что, несмотря на то, что рассматриваются различные толкования анализируемого понятия (персональные данные, персональная информация либо личная информация), приоритетным будет использование именно термина «персональные данные».

## 1.2 Правовая природа персональных данных и их категорирование

### 1. Природа персональных данных

Возникновение категории персональных данных в информационном праве неразрывно связано с концепцией защиты частной жизни. В условиях развития информационного общества неприкосновенность частной жизни всё чаще сталкивается с различными угрозами. Именно необходимость обеспечения адекватной защиты прав человека от информационных рисков обусловила появление идеи регулирования обращения персональных данных как особого вида информации, требующего специальной защиты. Персональные данные являются удивительным и, наверное, самым уникальным с точки зрения особенностей правового режима видом информации ограниченного доступа[36]. Следовательно, анализ юридической природы персональных данных невозможен без учёта правовых норм, касающихся неприкосновенности и уважения частной жизни[37].

---

[35] Например, США привыкли рассматривать защиту персональных данных с точки зрения прав на неприкосновенность частной жизни и законов о неприкосновенности частной жизни, в то время как большинство стран Европейского союза и Россия предпочитают концепцию персональных данных, а Китай обычно использует термин «персональная информация».

[36] *Минбалеев А.В.* Трансформация правового режима персональных данных// Устойчивое развитие России: правовое измерение: сборник докладов X Московского юридического форума: в 3 ч. Часть 1. М.: Издательский центр Университета имени О.Е. Кутафина (МГЮА), 2023. С.163.

[37] *Бундин М.В.* Персональные данные в системе информации ограниченного доступа: дисс… канд. юрид. наук. М., 2017. С. 14.

Значительное количество зарубежных авторов утверждают, что право на неприкосновенность частной жизни представляет собой неотъемлемый компонент системы прав личности. В эту систему также включаются право на жизнь, защита репутации, чести и достоинства индивида и частной жизни, личной неприкосновенности[38]. Ряд российских ученых в своих работах также поднимают вопрос о правовой природе персональных данных.[39]Автор полностью согласен с позицией И.А. Вельдера о том, что право на защиту персональных данных относится к сфере фундаментальных прав личности[40].

Согласно общей позиции китайских ученых, основным атрибутом персональной информации является идентификация. В то же время персональная информация обладает и другими особыми свойствами, обусловленными её различным содержанием и формами, включая чувствительность, конфиденциальность и социальность.

1) Идентификация. Персональная информация – это совокупность любой информации, которая может идентифицировать конкретное физическое лицо, охватывая физические, психологические, социальные и экономические аспекты и имея функциональное значение для определения личностных характеристик физических лиц и предсказания законов объективной социальной практики[41].

---

[38] *Beigner B.* La protection de la vie privee // Libertes et Droits fondamentaux. Paris: Dalloz, 2003. P. 161–163.

[39] Например, по мнению В.Н. Лопатина, «право на неприкосновенность частной жизни – это сложный по составу правовой институт, включающий в себя множество отдельных правомочий индивида», указывая на персональные данные как на институт охраны права на частную жизнь; другие ученые, говоря о соотнесении персональных данных и права на неприкосновенность частной жизни, сделали вывод, что они являются связанными между собой понятиями, но в то же время не тождественными. Например, И.А. Вельдер заявляет о персональных данных как о «комплексном и самостоятельном образовании» – новом правовом институте; Н.Г. Белгородцева в своей работе также разделяет идею «самостоятельности» персональных данных, но путем выделения правового института «защиты персональных данных, который носит межотраслевой комплексный характер». См.: *Бачило И.Л.* Информационное право / И.Л. Бачило, В.Н. Лопатин, М.А. Федотов. СПб.: Юридический центр Пресс, 2005. С. 220; *Бачило И.Л.* Информационное право / И.Л. Бачило, В.Н. Лопатин, М.А. Федотов. СПб.: Юридический центр Пресс, 2005. С. 243; *Вельдер И.А.* Система правовой защиты персональных данных в Европейском союзе: дисс. канд. юрид. наук: 12.00.10. Казань, 2006. С. 10; *Белгородцева Н.Г.* Теоретико-правовые аспекты защиты персональных данных: автореф. дис. канд. юрид. наук. М., 2012. С. 10–11; *Бундин М.В.* Персональные данные в системе информации ограниченного доступа: дисс… канд. юрид. наук. М., 2017. С. 25-26 и др.

[40]Схожую точку зрения можно найти и в исследовании Н.Г. Белгородцевой, которая также склонна рассматривать «защиту персональных данных» и «право на защиту персональных данных» как одну из разновидностей юридических гарантий конституционных прав человека, а также у А.С. Федосина. См.: *Вельдер И.А.* Система правовой защиты персональных данных в Европейском союзе: дис. канд. юрид. наук: 12.00.10. Казань, 2006. С. 33; *Федосин А.С.* Защита конституционного права человека и гражданина на неприкосновенность частной жизни при автоматизированной обработке персональных данных в Российской Федерации: автореф. дис. ... канд. юрид. наук: 12.00.14. Саранск, 2009. С. 7.

[41] *Ци Айминь.* Исследование законодательства о защите персональной информации // Юридическая наука Хэбэя. 2008. № 4. С. 15-33.

«Идентификация» должна быть присуща не только экономическим отношениям и стимулировать исключительно коммерческие цели ее развития, но и быть связана с гуманитарными и культурными задачами. [42] С точки зрения государств или международных организаций «идентификация» признается наиболее важным юридическим атрибутом персональной информации и рассматривается как необходимый элемент для ее защиты. Иными словами, сфера применения защиты личной информации зависит от того, включает ли она информацию, позволяющую идентифицировать конкретного лица. Только «идентифицируемая» или «идентифицированная» информация напрямую связана с нанесением ущерба личной информации или интересам конфиденциальности[43].

2) Чувствительность. Подавляющее большинство персональных данных обладают характеристиками чувствительности. «Чувствительность» описывает возможность того, что деятельность по обработке, в том числе использованию, персональной информации приведет к потенциальным угрозам или существенному ущербу для субъекта персональной информации. С точки зрения субъектного познания чувствительность отражает своего рода склонность к осознанию риска, заключающуюся в том, что субъекты, обладающие персональной информацией, не могут контролировать обработку своей собственной информации в современном обществе риска[44].

3) Конфиденциальность. В зависимости от сути данных фактически зависит, будет ли это режим конфиденциальности или открытый. [45] Персональные данные могут быть и открытыми в силу прямого указания в законе или воли субъекта персональных данных. Но субъект всегда вправе и ограничить доступ к его персональным данным, даже если ранее он их предоставлял во всеобщий доступ. Секретные сведения личной информации охраняются в режиме

---

[42] *Наумов В.Б.* Задача обеспечения тайны идентификации в информационном праве // Мониторинг правоприменения. 2019. №3 (32). С. 71.

[43] *Schwartz P.M.*, & Solove D.J. The PII Problem: Privacy and a New Concept of Personally Identifiable Information[J]. New York University Law Review, 2011,86(6): 1814-1894.

[44] *Defilippis A.J.* Securing Information Ships: Recognizing a Right to Privity in Fourth Amendment Jurisprudence[J]. The Yale Law Journal, 2006,115(5): 1086-1121.

[45] *Минбалеев А.В.* Новеллы законодательства о персональных данных // Университетские правовые диалоги: материалы Международной научно-практической конференции, 30–31 марта 2023 г. / под ред. Е.В. Титовой. – Челябинск: Издательский центр ЮУрГУ, 2023. С.108.

конфиденциальности. Секреты частной жизни или связанные с ней частное жизненное пространство также носят конфиденциальный характер[46]. То есть персональные данные содержат личную информацию, которая должна храниться в тайне. Утечка указанных данных может привести к таким негативным последствиям, как незаконная обработка персональных данных в системах искусственного интеллекта[47], мошенничество или вторжение в частную жизнь.

4) Социальность. В условиях развития активного использования больших данных и других цифровых технологий социальная природа личной информации становится все более очевидной. Как один из социальных ресурсов персональная информация обладает высокой эффективностью или полезностью, а ее надлежащая и разумная обработка может удовлетворить реальные потребности конкретных личных, социальных и общественных интересов.

**2. Категорирование (категоризация) персональных данных**

В ходе определения уровня безопасности и организации мероприятий, направленных на нейтрализацию угроз безопасности, приоритетное значение имеет засекречивание персональных данных, предусмотренное ФЗ о ПДн и Постановлением Правительства Российской Федерации № 1119[48]. Традиционно выделяется четыре категории персональных данных: персональные данные общей категории, общедоступные персональные данные[49], специальные категории персональных данных[50], биометрические персональные данные.[51] При этом

---

[46] *Чжан Синьбао.* Правовая защита права на неприкосновенность частной жизни. Пекин: Издательство "Массы". 2004. С. 16-17.

[47] *Минбалеев А. В.* Филоненкова В. А. Проблемы защиты персональных данных и цифрового профиля человека в сети Интернет в условиях пандемии // Вестник Южно-Уральского государственного университета. Серия : Право. 2020. Т. 20. № 3. С. 89.

[48] Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». // Собрание законодательства РФ. 2012. № 45. Ст. 6257.

[49] Общедоступные персональные данные являются таковыми в силу прямого указания в законе или решения субъекта персональных данных. Согласно ст. 8 ФЗ о ПДн «в целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных». См.: Федеральный закон от 27 июля 2006 г. № 152-ФЗ "О персональных данных" // Собрание законодательства Российской Федерации. 2006 г. № 31 (часть I). Ст. 3451.

[50] Это персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни. См. ст. 10 Федерального закона от 27 июля 2006 г. № 152-ФЗ "О персональных данных" // Собрание законодательства Российской Федерации. 2006 г. № 31 (часть I). Ст. 3451.

персональные данные общей категории – это обычные персональные данные, которые не отнесены ни к одной из других категорий, в отношении них распространяется общий режим законодательства о персональных данных.

Применительно к персональным данным обычно указываются номер телефона, имя, адрес, медицинская информация, адрес электронной почты и т.д. Один из китайских юристов разделил персональные данные на 13 категорий в зависимости от их «чувствительности» [52] . Причем, сведения о личности, информация об интимной жизни, биометрическая информация, информация о спорте и состоянии здоровья и информация о собственности признаются высокочувствительной информацией (Приложение 1).

С точки зрения конструкции информации, существует два типа персональных данных: единичная форма информации и составная форма информации. Первый тип личной информации в независимой форме может быть идентифицирован и привязан к конкретному физическому лицу, например: номер удостоверения личности, адрес регистрации домохозяйства, информация о местонахождении и т.д.; составная форма информации может представлять собой комбинацию однотипной персональной информации, обезличенной информации и анонимной информации, которая после обработки с помощью технологии больших данных может превратиться в «синтетическую» идентификационную карту, соответствующую требованиям клиентов[53].

Принимая во внимание требования правовой защиты безопасности персональных данных, китайский специальный закон, регулирующий институт персональной информации, устанавливает, что стандартом классификации персональной информации должна быть степень их чувствительности, т.е. персональные данные следует разделять на чувствительную и обычную

---

[51] Биометрические персональные данные – это сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных. См. ст. 11 Федерального закона от 27 июля 2006 г. № 152-ФЗ "О персональных данных" // Собрание законодательства Российской Федерации. 2006 г. № 31 (часть I). Ст. 3451.

[52] *Ху Вэньтао.* Концепция определения личной чувствительной информации в нашей стране // Юридическая наука в Китае. 2018. № 5. 235-254.

[53] *Чэнь Танфа.* Обсуждение дилеммы и правил защиты конфиденциальности в Интернете и среде больших данных // Цзинаньский Журнал. Философия и общественные науки. 2015. № 10. С. 126-130.

информацию.[54]

По мнению китайских ученых, целью системы защиты персональных данных является не защита самих персональных данных, а защита соответствующих прав и интересов при обработке персональных данных. Таким образом, чувствительная персональная информация носит ситуативные характеристики, и ее чувствительность часто варьируется в зависимости от различных факторов, связанных с ее обработкой, и различных защищаемых прав и интересов.[55] В связи с этим на уровне правового толкования и правоприменения определение чувствительной персональной информации должно основываться на оценочных суждениях граждан государства относительно чувствительности личной информации. Конечно, когда речь заходит о трансграничном распространении данных, определение чувствительной личной информации затрагивает факторы разных государств и регионов, т.е. критерии ее оценки различаются в разных государствах и регионах. При этом оценка чувствительной персональной информации не должна быть основана просто на односторонней позиции, а должна решаться на основе соответствующих соглашений, стандартов и двусторонних консультаций.[56]

Таким образом, с точки зрения правовой природы персональных данных в Китае и России выявлены как общие черты, так и существенные различия. Общим является признание особых свойств персональных данных, включая их чувствительность, конфиденциальность и социальную значимость, обусловленные разнообразием их содержания и форм выражения. Что касается различий, то в основе китайского подхода лежит критерий

---

[54] Согласно ст. 28 Закона КНР о защите персональной информации（2021）к чувствительной персональной информации относится персональная информация, утечка или незаконное использование которых может легко привести к ущемлению человеческого достоинства физического дица или угрозе его личной или имущественной безопасности, включая сведения о биометрических данных, религиозных убеждениях, об идентичности индивида, медицинском состоянии, финансовых счетах, о местонахождении и путях следования, а также персональную информацию о несовершеннолетних в возрасте до 14 лет. А такая информация, как ФИО, дата рождения, номер телефона, пользовательский контент и т.п., соответственно, относится к сфере обычных персональной информации.

[55] См.: *Дин Сяодун.* Пояснительная реконструкция системы защиты чувствительной персональной информации // Юридическая наука в Китае. 2025. № 2. С. 176.

[56] См.: *Пэн Юэ.* Модель регулирования конфиденциальности данных и ее отражение в торговом праве // Исследование в области права и бизнеса. 2022. № 5. С. 102-117; *Чжан Цзихун, Цай Юйцянь.* Международное регулирование трансграничной передачи чувствительной персональной информации // Гуансиские общественные науки. 2023. № 7. С. 107-118.

«идентифицируемости» (прямой или косвенной), который выступает центральным элементом в разграничении охраняемой информации и сферы её свободного использования.

Российское законодательство, определяя персональные данные как «любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу», формально задает сопоставимый по охвату нормативный критерий, акцентируя связь информации с конкретным лицом. Ключевое различие заключается не в абсолютной «широте» определения, а в системообразующем значении, которое придается этому критерию в правоприменительной практике, а также в методах его интерпретации контрольно-надзорными и судебными органами. Таким образом, российский подход позволяет шире определять круг сведений, относимых к персональным данным. С одной стороны, это усиливает гарантии защиты прав личности, с другой — может порождать дополнительную неопределённость в правоприменительной практике, в частности при определении применимости требований безопасности к сведениям, обладающим отдельными признаками персональных данных.

## 1.3 Теоретические основы публично-правового обеспечения безопасности персональных данных граждан

Защиту персональных данных как современную правовую концепцию следует рассматривать в контексте более ранней гуманитарно-правовой традиции, восходящей к идеям прав человека, личного достоинства и неприкосновенности частной жизни, которые получили важное развитие в период Великой французской революции. Именно тогда было впервые провозглашено понятие, подчеркивающее приоритет интересов отдельной личности над неограниченными правами государства. [57] Позднее сформировалась концепция «права на неприкосновенность частной жизни», одной из ключевых составляющих которой

[57] История защиты персональных данных. URL: https://searchinform.ru/resheniya/biznes-zadachi/zaschita-personalnykh-dannykh/realizaciya-zashchity-personalnyh-dannyh/istoriya-zashchity-personalnyh-dannyh/ (дата обращения: 17.10.2024).

стало право на защиту персональных данных. Данное неотъемлемое право личности обеспечивает защиту от незаконных посягательств как со стороны государства, так и со стороны третьих лиц. На пути развития к формированию современного понятия персональных данных данная концепция прошла этап существования в виде индивидуальных прав человека, включая право на получение информации, касающейся интересов личности, а также право на защиту данных, относящихся к частной жизни.

**1. Ценностная основа защиты персональных данных**

Человеческое достоинство и свобода информации формируют ценностную основу правовой защиты персональных данных. С одной стороны, личная информация отражает достоинство и интересы субъекта информации, а с другой стороны, в соответствии с принципом ценности свободы информации, обработка персональных данных считается обоснованной.[58] В связи с этим для решения проблемы ценностного выбора, с которой сталкивается регулирование оборота персональных данных, необходимо провести углубленный анализ и обсуждение с двух вышеперечисленных точек зрения.

1) Человеческое достоинство является одной из основ правовой защиты безопасности персональных данных. С момента зарождения юридической науки права и свободы человека стали предметом исследования множества отечественных и зарубежных ученых в различных научных направлениях. В процессе развития юридической науки существенно трансформировалось содержание теории прав и свобод человека, а также понимание ее природы и ключевых принципов.[59] Как достижение современной цивилизации, теория естественных прав и свобод человека акцентирует особое внимание на категории «достоинство» личности, наделяя её не только этико-философским, но и строго юридическим значением.

Достоинство личности является основным социальным и этическим принципом. Как отмечал И. Кант, природа человека — это достоинство, и человек

[58] *Ли И.* Ценностная дилемма и меры по защите персональных данных: с точки зрения разрешения конфликта между человеческим достоинством и свободой информации // Юридическая наука Хэбэя. 2013 №. 2. С. 2.
[59] *Мусалова З.М.* Понятие достоинства личности и эволюция представлений о нем // Юридический вестник ДГУ. Т. 24. 2017. № 4. С. 90.

должен стать самоцелью, а не средством [60], подчеркивая достоинство и благородство личности. Термин «личность» имеет наиболее абстрактное определение у Г.В.Ф. Гегеля: «Воля, существующая сама по себе, то есть абстрактная воля — это человек», или человек — это субъект, осознающий существование субъективности «я». Сущность личности заключается в том, что я как человек не только знаю ограничения и предписания самого себя как «человека», но и знаю, что я являюсь «чем-то бесконечным, универсальным и свободным»[61]. На самом деле это выражение содержит два аспекта личностной коннотации: во-первых, я могу стремиться к свободе и использовать ее как чистую цель; во-вторых, эта свобода может быть реализована и схвачена только в рамках чистого отношения к себе. Таким образом, Г.В.Ф. Гегель сформулировал личностное право в повелительной форме глагола как «Будь лицом и уважай других в качестве лиц» [62], что делает возможностью такую правоспособность как «не посягать на право на личность или на то, что вытекает из личности».

Личностное достоинство, по сути, включает в себя три вида ценностных значений: человек как самоцель и высшая ценность, ценность автономности личности и ценность ограничения государственной власти в отношении отдельных лиц. Если говорить более конкретно, то, во-первых, личностное достоинство подчеркивает, что человеческое существование и развитие являются фундаментальными ценностями. Следовательно, правовая система защиты персональных данных нуждается в разъяснении приоритетного принципа, согласно которому целью являются люди, а обработка персональных данных должна быть ограничены тем, чтобы не ущемлять интересы человеческого достоинства.

Во-вторых, личностное достоинство означает автономность человека[63], то

---

[60] *Кант И.* Критика практического разума. Перевод: Хань Шуйфа. Пекин: Коммерческая пресса. 1999. С. 93-96.
[61] *Гегель Г.В.Ф.* Основы философии права. Перевод: Фань Ян, Чжан Цитай. Пекин: Коммерческая пресса. 1961. С. 45.
[62] *Гегель Г.В.Ф.* Основы философии права. Перевод: Фань Ян, Чжан Цитай. Пекин: Коммерческая пресса. 1961. С. 46.
[63] *Ван Сюй.* Теория достоинства в конституционном праве и ее систематизация // Китайский юридический журнал. 2016. № 1. С. 37-55.

есть достоинство является результатом человеческой автономии, а ненадлежащее вмешательство в сферу этого рода автономии эквивалентно «недостойному». Эта ценность также может быть истолкована как свобода, равенство и самоопределение[64]. Иными словами, в сфере саморазвития индивиды не должны подвергаться вмешательству или вторжению внешних сил без очевидных законных причин, чтобы обеспечить условия для личностного саморазвития и самореализации. Если в процессе обработки персональных данных возникает тенденция относиться к субъекту информации как к объекту, это может привести к ущемлению личного достоинства человека.

В-третьих, реализация личностного достоинства требует ограничения неправомерного вмешательства и посягательства государственной власти. Отдельные лица не только имеют право требовать от государства выполнения своих обязательств по защите, но и имеют право ограничивать расширение государственной власти. Только тогда, когда государственная власть уважает автономию человека, признает цель человека главной ценностью и разумно ограничивает расширение своей власти и масштабы вмешательства, может быть по-настоящему реализовано личностное достоинство каждого человека.

Личностное достоинство занимает важнейшее место среди основных прав в правовых системах государств мира и в актах международных организаций.[65] Как

---

[64] *Ли Лей.* «Человеческое достоинство» в конституционном праве // Журнал Университета Сунь Ятсена. Общественные науки. 2002. № 6. С. 129-136.

[65] Как Всеобщая декларация прав человека, так и Хартия Европейского союза об основных правахпредусматриваю защиту «человеческое достоинства»; Статья 1 Основного закона ФРГ содержит положение о том, что достоинство человека неприкосновенно; уважать и защищать его – обязанность всякой государственной власти. Поставив защиту достоинства человека в начале Основного закона, учредители Конституции ФРГ ясно указали, что в устройстве Основного закона сначала идет человек, а затем государство; согласно статье 2 Конституции Российской Федерации, «Человек, его права и свободы являются высшей ценностью. Признание, соблюдение и защита прав и свобод человека и гражданина — обязанность государства»; Статья 38 Конституции Китайской Народной Республики также гласит, что «достоинство граждан Китайской Народной Республики неприкосновенны», и так далее. См.: Всеобщая декларация прав человека (полный текст). URL: https://www.coe.int/ru/web/compass/the-universal-declaration-of-human-rights-full-version- (дата обращения: 10.09.2024).

[65] Например, Всеобщая декларация прав человека (полный текст). URL: https://www.coe.int/ru/web/compass/the-universal-declaration-of-human-rights-full-version-; Хартия Европейского союза об основных правах. URL: https://normativ.kontur.ru/document?moduleId=1&documentId=178141&ysclid=m0vvr1474k903906578; Конституция Российской Федерации. (принята всенародным голосованием 12 декабря 1993 года с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 года) // Официальный интернет-портал правовой информации http://pravo.gov.ru, 06.10.2022; Конституция Китайской Народной Республики. URL: http://www.npc.gov.cn/c2/c30834/201905/t20190521_281393.html (дата обращения: 10.09.2024); Ушков, Д. Л. Конституционное право о «достоинстве личности» в РФ и ФРГ / Д. Л. Ушков. — Текст : непосредственный // Молодой ученый. 2016. № 5 (109). С. 529-531.

отмечали ученые еще в конце XIX – начале XX века, те правила о том, в какой мере отдельные лица имеют право обнародовать свои собственные данные, основаны не на правах личной собственности, а на более общем праве отдельных лиц на защиту от посягательств – части права на личность.[66]

Интересы, воплощенные в защите персональных данных, можно рассматривать как абстрактное право, то есть как личностное достоинство. Причина, по которой закон защищает личную информацию, заключается главным образом в том, что она содержит личные интересы субъекта информации, которые рассматриваются как личностное достоинство человека. Этот контекст также содержит основную логику и суть социалистической системы защиты прав человека с китайской спецификой в новую эпоху.[67]

Защита персональных данных, по сути, предполагает право человека на самоопределение и право на достоинство личности, с которыми он может справиться самостоятельно. Что касается внешнего формального элемента защиты персональных данных, то он не только содержит глубокую личностную ценность, но и отражает личностные интересы различных субъектов.[68] Право на персональные данные фактически демонстрирует свое доминирующее значение как своего рода личностное право. В этой связи защита персональных данных отвечает правомерным интересам защиты человеческого достоинства[69].

Следовательно, защита персональных данных должна основываться главным образом на базовом содержании человеческого достоинства и не должна рассматриваться как выходящая за рамки человеческого достоинства. Объектом защиты личной информации являются в основном духовные интересы. Если внешний мир ненадлежащим образом вмешивается в личные потребности, мысли

---

[66] *Луис Д. Брандейс и др.* Право на неприкосновенность частной жизни. Перевод: *Хуань Шэнкуй.* Пекин: Издательство Пекинского университета. 2014. С. 18-20.

[67] *Ван Сигэнь.* Ценность прав человека в представлении Си Цзиньпина о верховенстве закона // Восточное право. 2021. № 1. С. 37-46.

[68] Как сказал немецкий ученый Циммер, каждый должен демонстрировать целостность своей личности, скрывая свои собственные секреты, и в то же время использовать способ «секретного обмена различиями» для поддержания и формирования закрытого интимного отношения и пространства сообщества. См.: *Георг Циммер.* Социология: Исследование форм обобществления. Перевод: Линь Жунюань. Пекин: Издательство "Хуася". 2002. С. 264.

[69] То есть, я пользуюсь свободой неприкосновенности частной жизни и уважаю вашу этого рода свободу. См.: Costa-Cabral F., & Lynskey O. Family Ties: The Intersection between Data Protection and Competition in EU Law[J]. Common Market Law Review, 2017, 54 (1): 11-50.

и счастье человека, то возникают боль и страдания от того, что его лишают индивидуальности и достоинства. Как показали некоторые исследования, персональные данные являются ключевым средством и содержанием взаимодействия человека с другими субъектами общества[70]. Использование и совершение иных действий с персональными данными по своему усмотрению являются основной предпосылкой для свободного развития его личности. Самоконтроль персональных данных является необходимым условием для защиты человеческого достоинства в цифровую эпоху.[71]

Защита персональных данных, безусловно, требует ограничения государственной власти на посягательство на частную сферу. Ключ к обеспечению человеческого достоинства лежит в прояснении отношений между личностью и государством. В конституциях многих государств мира закреплено, что государство должно уважать и защищать личностные интересы. В зарубежной доктрине отдельные авторы говорят, что нет необходимости даже «выражать это вслух».[72]

По мнению автора, ограничение обработки персональных данных органами государственной власти сможет гарантировать право отдельных лиц на свою собственную информацию и контроль над ней, а также максимально способствовать сохранению «целостности» человеческого достоинства. Иными словами, ограничение использования личной информации государственными органами помогает смягчить ущерб, наносимый человеческому достоинству в результате постепенного вмешательства государства, правительственной структуры и других авторитарных организаций или отдельных лиц в частную жизнь отдельного индивида.[73]

Получается, что право на личностное достоинство, которым пользуются

---

[70] *Се Юаньян.* Ценность личной информации с точки зрения теории информации: обзор модели защиты прав на неприкосновенность частной жизни // Юридический журнал университета Цинхуа. 2015. № 3. С. 94-110.

[71] Там же.

[72] Так, Элен Ниссенбаум считает, что у общественности есть три основных требования к неприкосновенности частной жизни или интересам в области персональных данных: первое – ограничить слежку за гражданами и их использование государственными должностными лицами; второе – ограничить сбор и приобретение чувствительной, приватной или конфиденциальной информации; и третье – ограничить вмешательство государственной власти на то, что считается частной территорией. См.: *Nissenbaum H.* Privacy as Contextual Integrity[J]. Washington Law Review, 2004,79(1): 119-157.

[73] *Rubenfeld J.* The Right of Privacy[J]. Harvard Law Review, 1989,102(4): 737-807.

отдельные лица, включает в себя основные интересы в виде защиты частного пространства индивида от вторжения и его частной жизни от неправомерного вмешательства со стороны других лиц. Ограничение государственного вмешательства в частную жизнь отдельных лиц и обеспечение контроля отдельных лиц над их собственной информацией фактически эквивалентно признанию и уважению их субъективного статуса и сохранению личностной свободы.

Сохранение «целостности» человеческого достоинства должно быть направлено на защиту интересов его личности. Их нарушение неизбежно приведет к потере «целостности» субъекта персональных данных как человеческого существа.[74] Фактически, во всем мире большинство государств защищают личностное достоинство субъектов персональных данных, устанавливая баланс между законными интересами при использовании персональных данных и риском причинения вреда личности субъекта персональных данных.[75]

В связи с активным использованием больших данных ненадлежащая обработка персональных данных нарушает основные этические требования принципа «человек – это цель», что может легко привести к злоупотреблению личной информацией, превращению людей в инструменты и управлению данными, которые они создают. В то же время чрезмерное использование личной информации ослабит субъектность людей, и живая индивидуальная личность уступит место «цифровой биографии или атласу», ослабляя истинное «Я» человека и его способность принимать решения. Как отметил Ван Цзэцзянь, «неприкосновенность частной жизни представляет собой фундаментальный инструмент для обеспечения личной автономии и индивидуальности,

---

[74] Отдельные исследователи отмечают, что обычный сбор данных о транзакциях, все более активное автоматическое наблюдение в общественных местах, мониторинг рабочих мест, отслеживание интернет-трафика от файлов cookie до «кликов», «переключение программного обеспечения» для защиты прав интеллектуальной собственности и другие новые технологии привели к тому, что каждый должен стать «прозрачным человеком». См.: *Froomkin A.M.* The Death of Privacy? [J]. Stanford Law Review, 2000, 52(5): 1461-1543.

[75] *Post R.C.* Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of the Public Sphere[J]. Duke Law Journal, 2018,67(5): 981-1072.

направленный на сохранение человеческого достоинства».[76]

Вторжение в сферу частной жизни лица, нарушение её неприкосновенности, разглашение конфиденциальной информации, а также психический дискомфорт, боль или чувство стыда, вызванные данными действиями, представляют собой прямое посягательство на человеческое достоинство. Поэтому некоторые ученые отмечают, что мы всегда должны придерживаться требований верховенства закона о том, что «человек – это цель», рассматривать человеческое достоинство как высшую ценность в процессе развития информационных технологий нового поколения, умеренно регулировать обработку персональных данных и тщательно применять алгоритмы, искусственный интеллект и другие технологии для интеллектуального анализа данных в конкретных основных областях, чтобы укрепить субъектность человека, способствовать инклюзивному развитию многообразия человеческого и социального развития и, в конечном счете, уменьшить ущерб человеческому достоинству.[77]

2) Свобода информации выступает в качестве основы правовой защиты персональных данных. Подобно личностному достоинству, свобода информации также является одним из основных прав, общепризнанных конституциями различных государств. Она имеет прямое отношение к свободе выражения мнений, свободе общения, свободе прессы и т.д., а также имеет глубокую внутреннюю связь с правом знать, раскрытием информации и другими правами.[78]

Свобода – это врожденная добродетель человека, а также его естественное право. Проблема свободы актуальна и нуждается в глубоком философском исследовании. К этой теме обращались не только отдельные выдающиеся мыслители, но и целые философские течения, такие как марксизм, экзистенциализм, ибо свобода относится к числу вечных, подлинно философских

---

[76] *Ван Цзэцзянь.* Конкретизация прав личности и сферы их защиты. Право на неприкосновенность частной жизни (часть 1) // Журнал сравнительного правоведения. 2008. № 6. С. 1-21.

[77] *Хун Данна.* Корректировка конституционного значения алгоритмической дискриминации: на основе уважения человеческого достоинства // Политика и право. 2020. № 8. С. 27-37.

[78] *Цзян Юнфу, Хуан Лися.* Свобода информации, информационные права и публичная библиотечная система // Документы, информация и знания. 2005. № 1. С. 20-23.

проблем, заставляющих человеческую мысль работать с полной отдачей. [79] Новейшему определению свободы с точки зрения либерализма мы обязаны австрийскому правоведу, экономисту Фридриху Августу фон Хайеку.[80]

Из вышеизложенного можно сделать вывод, что свобода – это всегда ограниченная «вольность», которая должна быть признана и гарантирована законом. Как отмечала С.Г. Чубукова, «любые свободы имеют ограничения в случаях, когда они противоречат основным правам человека»[81]. В наше время личная информация как основной ресурс социального взаимодействия должна обладать как частными, так и социальными свойствами. В этой связи исследователи отмечают, что следует передать государству часть прав членов общества на их собственную информацию для удовлетворения потребностей различных интересов, таких как социальные обмены, национальное управление и саморазвитие.[82] Таким образом, свободу информации можно рассматривать как естественное состояние людей, которые свободно собирают, используют и распространяют информацию в законных рамках, что является концентрированным воплощением свободы человека в информационном обществе.

Свобода информации, по сути, содержит в себе такие основные ценностные значения, как информационное равенство, обмен информацией, эффективность информации и информационная справедливость.[83]

---

[79] Как сказал Ж.-Ж. Руссо, «люди рождаются свободными и равноправными» «человек рождается свободным, а между тем всюду он в оковах» «отказаться от своей свободы – значит отказаться от человеческого достоинства, от прав человека»; Шарль Луи Монтескье так и писал, что «свобода – это право делать все, что разрешено законом»; Во времена Робеспьера, свободой называли право человека делать все, что не вредит другим людям. См.: *Руссо Ж.-Ж.* Общественный договор. Перевод: Ли Пин-оу. Пекин: Коммерческая пресса. 2011. С. 4, 12, 34, 58; *Монтескье Ш.Л.* О духе законов (часть 1). Перевод: *Сюй Минлун.* Пекин: Коммерческая пресса. 2012. С. 184; Несвобода, Неравенство, Небратство. URL: https://doelectricsheepdream.wordpress.com/2022/01/05/несвобода-неравенство-небратство/ (дата обращения: 11.09.2024).

[80] Его взгляд на свободу описывается в его трудах «Конституция свободы» 1960 года и «Право, законодательство и свобода» 1973 года. Свободу Хайек в первой главе работы «Конституция свободы» определяет как отсутствие вмешательства и принуждения в человеческую жизнь – «Состояние человека, в котором он не подвергается принуждению на основании произвольных решений другого или других, часто определяется как «индивидуальная» или «личная» свобода. См.: Люди и идеи. Суть и происхождение свободы по Хайеку. URL: https://vk.com/wall-188471171_1716 (дата обращения: 11.09.2024).

[81] *Чубукова С.Г.* Правовые проблемы защиты генетической информации: субъектный подход // Вестник университета имени О.Е. Кутафина (МГЮА). 2020. №.5. С. 102.

[82] *Джингте Якобус* Норма. Личность. Общество - предпосылки права философии. Перевод Фэн Цзюня, Пекин: Юридическая пресса. 2001. С. 111.

[83] *Го Минлун.* О коммерциализации персональной информации // Юридический форум. 2012. № 6. С. 108-114.

Во-первых, свобода информации требует, чтобы субъекты информации и другие субъекты могли пользоваться равным статусом, равными возможностями и равной свободой распространения в практической деятельности, связанной с личной информацией. Эта ценность в корне отрицает информационную дискриминацию, включая неравное обращение в различных областях, таких как онлайн-покупки, здравоохранение, информационные услуги и государственное управление. На данный момент ценностная концепция свободы информации фактически согласуется с запретом «дискриминационного обращения» при защите персональных данных.

Во-вторых, свобода информации на самом деле ограничена и специфична в понимании социальной и публичной ценности информационных ресурсов при условии уважения личного достоинства субъекта персональных данных, что подчеркивает разумные обмены информационными ресурсами и данными между разными субъектами.

В-третьих, свобода информации, воплощая в себе представление о справедливости, которое предполагает эффективное распределение персональных информационных ресурсов исходя из предпосылки «наибольшего счастья наибольшего количества людей» и «экономического человека» (economic man), стремится к устойчивому развитию в распределении эффективности и защите личности.

Вышеупомянутые ценности в целом отражают своего рода ценностное ожидание от свободы информации к справедливости информации, то есть свобода информации, по сути, отражает состояние свободы в виде баланса и взаимности при приобретении и распространении персональных информационных ресурсов[84]. Особенно с наступлением эры больших данных персональные информационные ресурсы стали основным фактором производства, и их «редкость и эксклюзивность» становятся все более заметными, а «неконкурентное и неисключительное» использование этого рода ресурсов все больше становится ценностной привлекательностью, что неизбежно приводит к ценностному

[84] *Цзян Юнфу, Лю Синь.* Об информационной справедливости // Библиотека и информация. 2005. № 6. С. 2-5, 22.

конфликту между защитой личностного достоинства и реализацией свободы информации[85].

Считается, что свобода информации в основном включает в себя два вида юридических прав: во-первых, право граждан на свободу выражения мнений, включая свободу мысли и право искать, получать и выражать информацию[86]; во-вторых, право граждан знать, то есть свобода получать государственную информацию, включая активное раскрытие и самостоятельный доступ к такой информации.[87] Так, концепция права на свободу информации в современном обществе эволюционировала в право на защиту доступа к правительственной информации и ограничение государственного вмешательства[88], что сосредоточено в качестве своего рода ценностного призыва к «информированности и раскрытию информации». В настоящее время свобода информации также включает в себя такое возможное право, как право на использование социальных ресурсов.[89]

Свобода информации имеет важное современное значение для экономики данных и социального развития, что в основном отражается в следующих четырех аспектах.

Во-первых, свобода информации способствует свободному обмену персональными информационными ресурсами и данными, снижению транзакционных издержек и накоплению цифровой остаточной стоимости.[90] Чрезмерные ограничения на персональные информационные ресурсы напрямую

---

[85] *Post R.C, & Rothman J.E.* The First Amendment and the Right(s) of Publicity[J]. Yale Law Journal, 2020,130(1): 86-172.

[86] Джон Мильтон обсуждал моральные и правовые истоки свободы информации в работе «О свободе печати» еще в 1644 году, утверждая, что свобода выражения мнений связана со свободой мысли, доступом к знаниям и рациональному суждению, и подчеркнул, что запрещение свободы прессы бесполезно и недостижимо. См.: *Мильтон Дж.* О свободе печати. Перевод: У Чжичунь. Пекин: Коммерческая пресса. 1958. С. 1, 6.

[87] *Ван Сигэнь, Чэнь Яньгуан.* О праве знать // Правовая система и социальное развитие. 2003. № 2. С. 62-74; Хуан Цзянью. Право выражать свое мнение или право знать: изменения в значении понятия свободы информации // Китайский журнал журналистики и коммуникации. 2018. № 9. С. 116-127.

[88] *Brucker H.* Freedom of Information[M]. New York: Macmillan Co, 1949: 276.

[89] Согласно гипотезе Познера, ожидания людей в отношении интересов конфиденциальности в основном основаны на соображениях соотношения затрат и выгод; как субъект использования информации, так и сам информационный субъект испытывают потребность в получении наилучшей полезности в процессе свободного обмена информационными ресурсами. См.: *Posner R.A.* Privacy, Surveillance, and Law[J]. The University of Chicago Law Review, 2008,75(1): 245-260.

[90] Некоторые ученые также высказали аналогичную позицию: «Конфиденциальность и информационные ресурсы являются не только промежуточным товаром, но и могут быть непосредственно использованы для чисто социального потребления. Фактически, они могут быть использованы в качестве своего рода источника вклада для получения выгод и, таким образом, максимизации социального благосостояния». См.: *Алита Л. Аллен, Ричард К. Стоктон.* Право на неприкосновенность частной жизни в США: доктрина, прецедент и законодательство. Перевод: Фэн Цзяньмэй и др. Пекин: Издательство "Китайская демократия и право". 2019. С. 168.

влияют на эффективность транзакций и транзакционные риски и в конечном итоге увеличивают транзакционные издержки.

Во-вторых, свобода информации помогает реализовать право граждан на свободу выражения мнений, повышает прозрачность государственного управления и ограничивает нарушения со стороны государственных органов. Право на информацию, свобода информации и механизм раскрытия информации образуют взаимосвязанную систему. Если отсутствует возможность требовать раскрытия информации, право граждан на получение сведений остаётся преимущественно декларативным. В свою очередь, свобода информации предполагает не только доступ к сведениям, но и их распространение в пределах, допустимых законом. Соотношение этих категорий в целом выражает конституционный принцип обеспечения прав граждан и сдерживания публичной власти[91]. Кроме того, обеспечение свободы и открытости информации позволяет повысить прозрачность деятельности государственных органов и создать дополнительные гарантии против злоупотребления публичной властью[92].

В-третьих, свобода информации способствует укреплению доверительных отношений с обществом. Обмен персональными данными всё чаще выступает не просто как передача сведений о человеке, а как элемент доверительных отношений между индивидом, обществом и государством. В таких условиях персональные данные нельзя рассматривать исключительно через призму частного интереса: их использование затрагивает и более широкий общественный контекст. В связи с этим защита персональных данных должна постепенно выходить за пределы традиционной модели охраны индивидуальных прав и включать защиту социальных отношений доверия, формирующих основу современной цифровой коммуникации[93].

В-четвёртых, свобода информации способствует повышению эффективности социального управления. В условиях активного развития технологий больших

---

[91] *Го Даохуэй.* Право знать и система раскрытия информации // Цзянхайский академический журнал. 2003. № 1. С. 127-133, 207.

[92] *Стиглиц, Сун Хуалинь.* Свобода, право знать и публичный дискурс: роль прозрачности в общественной жизни // Глобальный юридический обзор. 2002. № 3. С. 263-273.

[93] *Waldman A.E.* Privacy as Trust: Sharing Personal Information in a Networked World[J]. University of Miami Law Review, 2015,69(3): 559-630.

данных информация всё чаще рассматривается как ключевой ресурс, а персональные данные используются в различных сферах, включая электронную торговлю, здравоохранение и научные исследования. При этом государство, обладая значительными организационными и техническими возможностями, выступает одним из наиболее влиятельных субъектов обработки персональной информации. В связи с этим открытость данных направлена не только на расширение информационного обмена, но и на стимулирование инноваций в сфере больших данных, а также на повышение качества социального и государственного управления[94].

Таким образом, обеспечение безопасности персональных данных и их обработка представляют собой во многом симбиотические отношения, но при этом возникают серьёзные конфликты интересов, которые неизбежны из-за различий в их ценностных позициях. Основная ценность первой заключается в человеческом достоинстве, а вторая – в свободе информации. Эти две ценности имеют особое значение в различных ситуациях. В результате правовая защита персональных данных сталкивается с дилеммой: ограничение обработки личной информации другими лицами в целях поддержания личного достоинства субъекта информации будет препятствовать реализации свободы информации, а разрешение другим лицам свободно использовать персональные данные в целях реализации свободы информации может нанести ущерб личностному достоинству субъекта персональных данных. Это требует оценки конфликта интересов между «защитой» и «обработкой» (прежде всего использованием) и возможности координации между ними.

**2. Теоретико-правовые основы обеспечения безопасности и защиты персональных данных**.

В настоящей диссертации акцент делается на исследовании публично-правовых мер обеспечения безопасности персональных данных, а не на мерах защиты персональных данных. В литературе существуют различные подходы к

---

[94] *Hardy K., & Maurushat A.* Opening up Government Data for Big Data Analysis and Public Benefit[J]. Computer Law & Security Review, 2017, 33(1): 33-37.

соотношению категорий «меры безопасности» и «меры защиты». Некоторые авторы не видят принципиальной разницы между этими категориями[95]. Полагаем, что необходимо все-таки их различать. В литературе отмечается, что, поскольку «меры безопасности направлены на охрану самой безопасности, то их целью является предупреждение возникновения самих угроз и создание всех необходимых условий для их нейтрализации. В свою очередь, целью мер защиты следует признать противодействие тем из них, что уже наступили»[96]. Обеспечение безопасности персональных данных предполагает формирование состояния защищенности персональных данных, не допускающее несанкционированный доступ к ним третьих лиц. Это состояние, при котором не происходят незаконный оборот и другие незаконные действия с персональными данными субъекта. Обеспечение безопасности персональных данных представляет собой совокупность правовых, организационных, технических и иных мер, направленных на установление состояния защищенности персональных данных, при котором отсутствует несанкционированный доступ к ним третьих лиц и не происходит их незаконная обработка. Меры защиты, напротив, связаны с реагированием на уже совершённое нарушение прав субъектов персональных данных. Однако в отношении персональных данных имеется очень важная особенность. Хотя персональные данные, как правило, относятся к информации ограниченного доступа, в определённых случаях они могут быть открытыми, в частности если субъект персональных данных сам принимает решение об их раскрытии. В этом случае, если персональные данные будут разглашены и будут предприняты меры защиты, то это не помешает субъекту требовать обеспечения конфиденциальности в дальнейшем в отношении раскрытых персональных данных. В связи с этим любые меры защиты в данном случае могут рассматриваться и как меры, направленные на обеспечение безопасности персональных данных, поскольку они обеспечивают принятие мер, позволяющих

---

[95] См.: *Щедрин Н.В.* Введение в правовую теорию мер безопасности. Красноярск: Изд-во Красноярского гос. ун-та, 1999. С. 47.

[96] *Умрихина Е.И.* Меры безопасности в российском праве, их отличие от мер защиты и мер контрольно-предупредительного воздействия. URL: https://cyberleninka.ru/article/n/mery-bezopasnosti-v-rossiyskom-prave-ih-otlichie-ot-mer-zaschity-i-mer-kontrolno-predupreditelnogo-vozdeystviya (дата обращения: 12.12.2025).

в дальнейшем обеспечивать конфиденциальность и безопасность персональных данных, то есть обеспечивать состояние защищенности на более высоком уровне. Соответственно, когда мы говорим об обеспечении безопасности персональных данных, то мы предполагаем решение задачи по недопущению нарушения прав субъектов персональных данных.[97] Меры защиты в этом случае имеют особое юридическое значение, поскольку их не стоит полностью отождествлять с мерами безопасности, но следует рассматривать как неотъемлемую их часть в рамках общесистемного подхода понимания обеспечения безопасности персональных данных. Меры защиты персональных данных ликвидируют наступившие угрозы, например, в связи с утечкой персональных данных, но при этом выступают и мерами, направленными на дальнейшее обеспечение безопасности, то есть состояние защищенности прав субъекта персональных данных, предотвращая возможность их дальнейшей незаконной обработки, поскольку субъект персональных данных может быть заинтересован в дальнейшей конфиденциальности этих данных в отношении других лиц.

Развитие систем и технологий управления сопровождается развитием теории информационного пространства [98] как инструмента поддержки управления. Наряду с технологией информационного пространства развивается технология информационного поля[99] также как инструмента управления. Информационное пространство и информационное поле являются реалиями, в которых развивается социальная кибернетика[100]. Социальная кибернетика произошла из применения

---

[97] *Ван Гуанлун.* Механизм административно-правового регулирования защиты персональных данных в Китае: состояние, недостатки и путь решения. // Вестник Московского университета. 2024. Серия 11. Право. Том 65. № 4. С. 204-232.

[98] См.: *Tsvetkov V. Ya.* Information Space, Information Field, Information Environment // European researcher. 2014. № 8-1 (80):1416-1422; *Ожерельева Т.А.* Информационное пространство как инструмент поддержки принятия решений // Славянский форум, 2016. № 4 (14). С.169-175.

[99] *Кудж С.А.* Информационное поле: Монография. М.: МАКС Пресс, 2017. 97 с.; *Майоров А.А.* Информационное поле // Славянский форум. 2013. № 2(4). С.144-150.

[100] Первое упоминание термина «кибернетика» содержится в научном труде Андре-Мари Ампера «Опыт о философии наук». Великий французский физик, математик и естествоиспытатель определил кибернетику как науку об управлении государством, призванную обеспечивать его жителям разнообразные блага. Современная трактовка термина была предложена американским математиком, одним из основоположников теории искусственного интеллекта Норбертом Винером. Он описывал кибернетику как науку, изучающую общие закономерности управления и передачи информационных данных в живых организмах, машинах и обществе. См.:Кибернетика: история развития и применение в наше время. https://gb.ru/blog/kibernetika/ (дата обращения: 13.09.2024).

технической кибернетики в социологии.[101] Выбор модели верховенства закона для защиты персональных данных – это классический вопрос, то есть «Кто будет субъектом защиты»? В связи с этим в юридических кругах последовательно сформировались две теоретические точки зрения: «персональная кибернетика» и «социальная кибернетика», которые также могут быть поняты как две основные модели «защиты на основе прав» и «защиты на основе власти».[102]

С точки зрения «персональной кибернетики», субъекты персональных данных должны стремиться к самоопределению и контролю над своей собственной информацией на основе индивидуальных прав, а также они должны признавать, определять и защищать личные и имущественные интересы, связанные с персональными данными, и обеспечивать им абсолютную защиту. Однако, согласно позиции «социальной кибернетики», общедоступные свойства персональных данных определяют, что объем и степень защиты персональной информации должны подвергаться необходимым ограничениям, а использование и совершение иных действий с персональными данными должны определяться не личной волей, а общественными привычками или законами.[103]

Однако полагаем, что сегодня явно есть необходимость подвергнуть критике ценностный конфликт между этими двумя моделями «персональной кибернетики» и «социальной кибернетики» для того, что позволяет одновременно заложить основу для последующей формулировки концепции сбалансированного регулирования.

1) Значение «персональной кибернетики». Существует два основных теоретических источника самоконтроля или личного контроля за защитой личной информации: один – это европейская теория права на информационное самоопределение, основанная на защите человеческого достоинства; другой – американская теория конфиденциальности информации, основанная на защите

---

[101] *Цветков В.Я., Рогов А.И., Титов Е.К.* Социальная кибернетика в цифровой трансформации общества // ИТ-СТАНДАРТ. 2021. № 1 (26). С. 4.

[102] См.: *Гао Фупин.* Защита персональных данных: от персональной кибернетики к социальной кибернетике // Китайский юридический журнал. 2018. № 3. С. 97-101; *Цуй Гобин.* Основная теория ограниченной эксклюзивности больших данных // Китайский юридический журнал. 2019. № 5. С. 3-24.

[103] *Ван Сисинь.* Национальные обязательства по защите персональной информации и их разъяснение // Юридическая наука в Китае. 2021. № 1. С. 145-166.

свободы человека. Для удобства обсуждения эти две теории в совокупности можно обозначить «персональной кибернетикой».

Следует отметить, что вышеупомянутые две теории в целом придерживаются ценностного положения о том, что люди имеют право контролировать свою собственную информацию и доминировать над ней в целях защиты и реализации своего личного достоинства и свободы. Это конкретно проявляется в следующем.

а) Теория права на конфиденциальность информации. Конфиденциальность информации включает в себя следующие три основных аспекта:

Во-первых, в какой степени люди контролируют свою собственную информацию? Считается, что конфиденциальность – это возможность отделить себя от других с точки зрения физического пространства, частной информации и личных интересов и «скрыть» себя, исключив такие нежелательные действия в отношении себя, как подглядывание, иное использование личных данных, вторжение в частное пространство и т.п. [104]

Во-вторых, какими правами обладают отдельные лица в отношении своей собственной информации? С точки зрения природы прав, в дополнение к правам личности, право контролировать личную информацию как своего рода собственность является еще одним важным понятием, то есть «право контролировать» считается своего рода правом на собственность или имущественным правом, которое выражает фактическое решение человека относительно своей собственной личности, поэтому этого рода контрольное право рассматривается как расширение прав личности.[105] Исходя из этого, считается, что личная информация возникает в процессе развития личности, и в результате отдельные лица имеют право обладания на свою информацию.

В-третьих, какими конкретными личностными или имущественными интересами пользуются отдельные лица в отношении своей собственной информации? Основа прав на неприкосновенность частной жизни заключается в

---

[104] То есть «конфиденциальность – это контроль за личной информацией, позволяющий гарантировать, когда и кем мы будем восприняты», или «конфиденциальность – это состояние существования, при котором люди защищены от ненужного доступа или контактов со стороны других». См.: *Parker R.B.* A Definition of Privacy[J]. Rutgers Law Review, 1974,27(1): 275-296; O'Brien, D.M. Privacy, Law, and Public Policy[M]. New York: Praeger Publishers, 1979: 15-16.

[105] *Westin A.F.* Privacy and Freedom[M]. New York: Atheneum Press, 1967: 324.

доминирующем праве физических лиц контролировать личную информацию. Право на конфиденциальность информации не ограничивается предотвращением получения нашей личной информации другими лицами, оно должно быть расширено, чтобы мы могли сами контролировать обработку личной информации[106].

Таким образом, фундаментальная ценность права на неприкосновенность частной жизни заключается в защите человеческого достоинства и свободы.

Право на неприкосновенность частной жизни изначально понималось не как имущественное право, а как составная часть личных прав человека. Оно выражает возможность лица самостоятельно определять границы вмешательства в его личное пространство, частные дела, интимную сферу и информацию о себе. Поэтому данное право тесно связано с человеческим достоинством, свободой личности и её информационным самоопределением. Важно подчеркнуть, что содержание права на неприкосновенность частной и личной жизни охватывает также возможность лица использовать свои персональные данные и распоряжаться ими в пределах, предусмотренных законом. [107] И право на неприкосновенность частной жизни предполагает уважение к личной сфере человека, включая те эмоциональные и доверительные связи, которые имеют значение для поддержания близких отношений. В данном контексте защита частной жизни выражается прежде всего в недопустимости раскрытия сведений личного характера без согласия лица, к которому они относятся. Сохранение конфиденциальности таких сведений позволяет человеку самостоятельно определять пределы доступа других лиц к его частной сфере и тем самым контролировать характер своих личных отношений.[108] Следовательно, ценность конфиденциальности заключается в создании условий для гармоничного развития межличностных и социальных отношений за счёт установления пределов доступа к сведениям личного и интимного характера. В этом контексте

[106] *Fried C.* Privacy. Yale Law Journal, 1968, 77(3): 475-493.
[107] *Сычева М. И.* Проблемы правового регулирования защиты персональных данных в сети Интернет // Международный журнал гуманитарных и естественных наук. 2022. № 10–3 (73). С. 175.
[108] Джули Иннес считает, что «интимность» объединяет три сферы – информацию, доступ и самоопределение, то есть содержание приватности включает в себя информацию, доступ и решения в интимных отношениях. См.: *Inness J.* Privacy, Intimacy, and Isolation[M]. New York and Oxford: Oxford University Press, 1992: 56.

конфиденциальность выступает средством контроля над взаимодействием с другими лицами, распространением информации о себе и реализацией самоопределения[109] в пределах частной сферы.

В-третьих, право на неприкосновенность частной жизни подчеркивает важность определения границ между публичной и частной сферами и либерально-демократического порядка. В большинстве случаев, если индивид не может гарантировать ограниченный доступ к секретам своей частной жизни, он теряет свое личное достоинство и свободу, и в то же время невозможно реализовать требование «неприкосновенности». В этой связи самоопределение и секреты тесно связаны.[110]

Система регулирования конфиденциальности информации, основанная на принципах человеческого достоинства и свободного развития личности, закрепленных в конституционном праве на неприкосновенность частной жизни, обеспечивает автономию индивидов в частной сфере. Это позволяет им принимать решения о жизни без внешнего вмешательства и реализовывать право на самоопределение в отношении своей персональной информации.

б) Теория информационного самоопределения. Европейские государства уделяют пристальное внимание защите персональных данных с позиций соблюдения личностного достоинства. Данная концепция включает два ключевых аспекта: право на самоконтроль персональных данных и регулирование процессов их обработки, что подразумевает возможность самостоятельного определения границ распространения информации о себе. С развитием информационных технологий, начиная с 1960-х годов, сбор, обработка персональных данных всё чаще стали осуществляться с применением компьютерных систем. При этом субъект персональных данных фактически потерял контроль или доминирование над этим процессом, что привело к резкому ухудшению субъективности и автономии индивида.[111] Именно в этом контексте традиционная система защиты «от вмешательства других лиц» начала активно стремиться включить в себя право

---

[109] *Rachels J.* Why Is Privacy Important? [J]. Philosophy & Public Affairs, 1975, 4(4): 323-333.
[110] *Gavison R.* Privacy and the Limits of Laws[J]. Yale Law Journal, 1980,89(3): 421-471.
[111] *Ши Цзяю*. Законодательство о защите персональных данных в онлайн-среде // Журнал Сучжоуского университета. Философия и общественные наука. 2012. № 6. С. 85-96.

«эффективно контролировать персональные данные и доминировать над ними»[112].

Общепризнано, что «уважение частной жизни» является правовой основой и целью защиты персональных данных в Европейском Союзе. Данное положение конкретно формулируется в Конвенции Совета Европы от 1981 года[113]. Далее Директива 95/46/ЕС установила минимальные стандарты и нормативные требования для правовой защиты персональных данных в государствах-членах ЕС. Право на информационное самоопределение было впервые закреплено в правовой системе Германии, где его фундаментом выступает принцип личностного достоинства. [114] С юридической точки зрения, право на информационное самоопределение вытекает из прав, содержащихся в пункте 1 статьи 1 «Человеческое достоинство» и пункте 1 статьи 2 «Общие права личности» Основного закона Германии. [115] Общие правила защиты данных, обнародованные Европейским союзом в 2016 году, добавили права субъектов персональных данных, такие как право на удаление и переносимость данных[116], чтобы еще больше отразить уважение к людям.

Представляется, что право на информационное самоопределение изменило традиционную модель защиты персональных данных, основанную на принципе

---

[112] *Хэ Сюйсюй.* Право на информационное самоопределение персональных данных в сравнительном правоведении // Журнал сравнительного правоведения. 2013. № 2. С. 61-76. [

[113] То есть, Конвенция о защите физических лиц в отношении автоматической обработки персональных данных, принятой Европейской комиссией в 1981 году, направлена на защиту основных прав и свобод людей, уважение частной жизни и содействие свободному обмену информацией. **См.:** Юридический институт Цзиндуна. Хартия ЕС: Обзор и практические рекомендации Общего регламента по защите данных (GDPR). Пекин: Юридическая пресса. 2018. С. 14.

[114] В «Деле о переписи населения» 1983 года Федеральный Конституционный суд Германии впервые использовал концепцию «права на информационное самоопределение» в форме судебной практики, подтвердив право на информационное самоопределение отдельно от общих конституционных прав личности. Суд интерпретировал это фундаментальное право, как наделяющее любого индивидуума так называемым “informationelles Selbstimmungsrecht”, т.е. базовым правом принимать решения относительно сообщения, передачи и использования своих персональных данных. Но также Конституционный суд в отношении данного права самоопределения признал наличие его определенных пределов. Преобладающие интересы общества в целом должны иметь возможность допускать ограничения этой персональной свободы. См.: *Горелихина О.А., Шлиньков А.А.* Правовая защита персональных данных в Германии // Вопросы экономики и права. 2012. № 3. С. 322.

[115] Согласно Основному закону Федеративной Республики Германии, «Достоинство человека неприкосновенно» (пункт 1 статьи 1); «Уважать и защищать его – обязанность всей государственной власти. Каждый имеет право на свободное развитие своей личности в той мере, в какой он не нарушает прав других и не посягает на конституционный строй или нравственный закон» (пункт 1 статьи 2). См.: Полный текст. Основной закон Федеративной Республики Германии. URL: https://www.1000dokumente.de/?c=dokument_de&dokument=0014_gru&object=translation&l=ru (дата обращения: 15.09.2024).

[116] Регламент (ЕС) 2016/679 Европейского парламента и Совета О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных и отмене Директивы 95/46 / ЕС (Общие правила защиты данных) от 27 апреля 2016 года. URL: https://ogdpr.eu/ru/gdpr-2016-679?ysclid=m12yub98pp94513030 (дата обращения: 15.09.2024).

свободы информации, но в то же время необходимо соблюдать баланс интересов между защитой человеческого достоинства и защитой свободы информации. На ранних этапах защиты персональных данных в Германии ограничения или даже запреты на сбор, обработку конкретной личной информации требовали проверки того, были ли обоснованные ожидания соблюдения интересов конфиденциальности. Суть этого заключается в предотвращении риска нарушения личностных или имущественных интересов.[117]

В рамках информационного самоопределения правовая система защиты персональных данных пытается установить способ защиты интересов конфиденциальности, основанный на праве контролировать поток личной информации. Правила обработки персональных данных трансформировались из принципа свободы поведения в направлении «контроля собственной информации субъектом данных», при этом организации, осуществляющие обработку персональных данных, обязаны предоставлять четкие и достаточные правовые основания для своих действий.

В целом, в разных государствах мира существуют различные модели правовой защиты персональных данных, но в основе своей они основаны на праве контроля индивида над своей собственной информацией и праве на самоопределение для реализации своего личностного достоинства и свободы. Основные характеристики заключены в трех аспектах:

Во-первых, защита персональных данных основывается на конституционном принципе человеческого достоинства и фундаментальных правах на свободу. Она направлена на предотвращение злоупотреблений со стороны государственной власти и подчеркивает важность сохранения личностного достоинства.

Во-вторых, право на неприкосновенность частной жизни и право на информационное самоопределение эволюционировали от пассивной защиты личностных прав к активному обеспечению контроля над собственной информацией. Это позволяет субъектам управлять своими персональными

---

[117] *Ян Фан.* Защита частной жизни в общих правах личности в Германии: ограничения на концепцию «самоопределения» в соответствии с принципом свободы информации // Восточное право. 2016. № 6. С. 104-116.

данными в рамках установленных законодательных норм.

В-третьих, данные теоретические положения не рассматривают персональные данные как объект абсолютного владения и контроля индивидуума. Вместо этого они используют контроль над персональными данными как механизм защиты личностного достоинства субъекта информации. Иными словами, цель защиты персональных данных заключается в защите основных прав человека, а не в предоставлении ему исключительного права распоряжаться своими персональными данными.

2) «Социальная кибернетика» в связи с активным внедрением и использованием технологий больших данных. Персональные данные обладают как частными, так и отличительными социальными свойствами. Персональные информационные ресурсы несут в себе не только интересы личности и ресурсы, которые могут быть разделены с помощью системы собственности, но и социальные интересы, и общественную заинтересованность с атрибутами социального взаимодействия, совместного использования.[118]

Так, повреждение персональных данных фактически происходит по механизму «противоправные действия – повреждение элементов личной информации – ущерб личностной собственности или общественным интересам». В связи с активным внедрением и использованием технологий больших данных информация отдельного человека практически не имеет экономической ценности, и для достижения эффективности распределения ресурсов необходимо преобразовать огромные объемы личной информации в данные. В то же время обработка государством персональных данных также помогает обеспечить точное и разумное управление и, в конечном счете, повысить общественное благосостояние. По сравнению с другими объектами прав и интересов, персональные данные представляют собой систему структуры интересов, состоящую из множества интересов и совокупности ценностей, включая личные интересы, социальные интересы и публичные интересы общества. Следовательно,

---

[118] *Се Хунфэй.* «Ущерб» в составе деликтной ответственности за утечку персональных данных: о концепции ущерба в рисковом обществе // Журнал Национальной академии прокуроров. 2021. № 5. С. 21-37.

логической отправной точкой для защиты персональных данных должно быть взвешивание интересов защиты личной информации и ее обработки, а не создание абсолютно исключительного права на защиту персональные данные.

В контексте экологии больших данных ученые разных государств постепенно начали принимать во внимание согласование личных ценностей и социальных норм и на этой основе стремиться к сбалансированному регулированию интересов в области обработки персональных данных и обеспечения их безопасности.[119] «Социальная кибернетика» утверждает, что индивидуальность – это только одна сторона личной информации, а социальная природа, связанная с другими лицами и общественными интересами, – ее более существенная сторона. Необходимо стремиться к порядку социального регулирования, обеспечивающему свободный поток личной информации, эффективную защиту личной информации и баланс интересов между ними, чтобы сохранить, продвигать и наследовать цивилизацию неприкосновенности частной жизни.[120]

Есть три основные причины, по которым предлагается идея «социальной кибернетики»: во-первых, институциональные механизмы в рамках персональной кибернетики могут легко привести к приватизации прав на личную информацию, что нарушает объектный признак личной информации как «инструмента» для практической деятельности в социальной сфере; во-вторых, «персональная кибернетика» привела к полному доминированию обработки персональной информации отдельными лицами, что нарушает основные принципы обработки персональной информации в условиях использования больших данных; модель верховенства права в рамках «персональной кибернетики» может не обеспечивать достаточную защиту персональных данных. После сбора персональной информации она де-факто выходит из-под контроля со стороны отдельного лица и может находиться под контролем только определённых субъектов, которые

---

[119] Как сказал Шварц, необходимо содействовать разумному сбору, обработке и распространению личной информации иерархическим и контекстуальным образом и в то же время обеспечивать максимальную защиту личностного достоинства и свободы человека. См.: *Schwartz P. M.* Privacy and Democracy in Cyberspace[J]. Vanderbilt Law Review, 1999, 52(6): 1609-1702.

[120] *Гао Фупин.* Защита персональных данных: от персональной кибернетики к социальной кибернетике // Китайский юридический журнал. 2018. № 3. С. 97-101.

используют данную информацию в своих целях.[121]

Следует подчеркнуть, что в предыдущих концепциях ценностной парадигмы, которая акцентировала внимание на самоконтроле персональной информации с позиций прав индивидуума, недостаточно учитывался аспект социального контроля в рамках социальной кибернетики. Однако в сценарии больших данных социального контроля в отношении персональных данных избежать не удастся. В то же время существует тенденция к «абсолютному социальному контролю», которая также заслуживает внимания. Идея о том, что полномочия по принятию решений в отношении персональных данных полностью передаются государству или обществу, по сути, является разновидностью «социального авторитаризма». На данный момент точка зрения китайского ученого Дин Сяодуна более нейтральна. Он считает, что защита персональных данных должна быть контекстуализирована: необходимо признать общественную ценность передачи персональных данных, а также необходимо усилить их частноправовую защиту и публично-правовое регулирование рисков в целях защиты личной информации.[122]

Получается, что «социальная кибернетика» отрицает полное и абсолютное право индивидов свободно распоряжаться персональными данными при любых обстоятельствах, и в то же время она также выступает против мощного контроля личной информации со стороны государства во имя «общественных интересов». Другими словами, два вышеперечисленных интереса (личные и общественные интересы) в области контроля за персональной информацией должны быть скоординированы и сбалансированы.

3) Теоретическая основа защиты персональных данных заключается в построении механизма обеспечения баланса интересов. Концепции «персональной кибернетики» и «социальной кибернетики» относятся к категории юридического регулирования защиты персональных данных. Оба теоретических подхода направлены на признание, определение и защиту прав и интересов, связанных с персональными данными, через систему юридических инструментов,

---

[121] *Цуй Гобин.* Основная теория ограниченной эксклюзивности больших данных // Китайский юридический журнал. 2019. № 5. С. 3-24.

[122] *Дин Сяодун.* Дилемма и выход из частноправовой защиты персональных данных // Китайский юридический журнал. 2018. № 6. С. 194-206.

а также на обеспечение и развитие упорядоченного управления обменом личной информацией.

Следовательно, необходимо не только защищать личностное достоинство, закрепленное в персональных данных, но и обеспечивать их законную, справедливую и рациональную обработку. Для этого требуется разработка системы регулирования, основанной на балансе интересов субъектов. Данная система должна способствовать соблюдению действующего законодательства в области защиты персональных данных, подтверждать приоритет ценности личностного достоинства и предупреждать возможные конфликты интересов. Иными словами, с учетом интересов свободы информации следует разработать рациональную систему интеграции интересов и механизм правовой поддержки для достижения оптимального баланса между защитой безопасности персональных данных и обеспечением доступа к информации.

В рамках данной системы необходимо выделить следующие основные теоретические положения:

1) Сохранение «целостности личностного достоинства» является первой существенной ценностью защиты персональных данных.

Основной задачей обеспечения баланса интересов в области защиты персональных данных является взвешивание и подтверждение ранжирования двух ценностей – личностного достоинства и свободы информации. С точки зрения институциональной справедливости, определенная правовая система должна преследовать основную ценность или конкретные институциональные интересы, что оказывает глубокое влияние на выживание и развитие указанной системы.[123]

Основной ценностью правовой системы по защите персональных данных может быть только «сохранение свободы информации при обеспечении человеческого достоинства», то есть человеческое достоинство должно занимать «приоритетное положение» в системе ценностей законов. Лишь при обеспечении приоритетной защиты личного достоинства субъекта персональных данных можно в дальнейшем заложить основу для рационального использования

[123] *Лян Шаншан.* Теория затрат и выгод. Пекин: Издательство Пекинского университета. 2021. С. 163.

информации другими лицами и добиться социального прогресса.[124] Персональные данные несут в себе личностное достоинство субъекта личной информации, что является основой для существования и функционирования персональной информации в практике общества: с одной стороны, персональные данные генерируются отдельными лицами в ходе их частных действий в сфере повседневной жизни и представляют собой совокупность информации, преобразованной личной волей и воспринимаемой внешним миром; с другой стороны, как только персональная информация сгенерирована, она становится медийным символом в социальной сфере, имеющим ценность поддержания социального взаимодействия, и в то же время она становится объектным ресурсом, имеющим ценность обмена и использования.

Независимо от того, что персональные данные используются как медийный символ или как ресурс обмена, их ценность заключается в практичной личности человека. Иными словами, персональная информация в социальных целях может использоваться как своего рода капитал в экономической, культурной и политической сферах, но независимо от того, в какую сферу личная информация попадает, она имеет свойство конфиденциальности, то есть свойство «человек – это цель».

В процессе персонификации имущественные интересы также являются продолжением личностной ценности и также могут стать объектом защиты со стороны правовой системы в сфере персональных данных. Индивидуальные интересы являются отправной точкой и конечным пунктом для обеспечения баланса интересов в области защиты персональных данных. «Величайшее счастье наибольшего числа людей», по сути, основано на личных интересах как отправной точке и точке опоры. Персональная информация не может быть узко понята как «национальная или социальная», либо она существует независимо от отдельных лиц в силу социальных и публичных интересов.

В то же время, персональные данные, несомненно, имеют экономическую

---

[124] *Ли И.* Ценностная дилемма и меры по защите персональных данных: с точки зрения разрешения конфликта между человеческим достоинством и свободой информации // Юридическая наука Хэбэя. 2013 №. 2. С. 2-7.

ценность. Особенно в связи с активным использованием технологий больших данных, ценность «прав собственности», содержащихся в персональных данных, несомненно, полностью объяснена. Иными словами, в процессе персонификации контроля за персональными данными необходимо учитывать вопросы эффективности. Конечно, защита личной информации должна соответствовать основной цели, которая заключается в более эффективном обеспечении счастливой жизни людей. Это требует, чтобы субъекты персональных данных не могли быть исключены из системы распределения благосостояния в рамках информационной экономики персональных данных. В противном же случае это может привести к структурному «чувству лишения неприкосновенности частной жизни» [125] в обществе или к трагедии с персональными информационными ресурсами, а также к нарушению основополагающей ценности справедливости в правовой системе.

Таким образом, в связи с внедрением больших данных необходимо признать, что персональные данные – это объект, который может быть активно использован. В то же время следует признать их фундаментальную ценность (т.е. «личная информация – это объективизация человеческого достоинства и свободы»), а также придерживаться принципа приоритетности личностных интересов при одних и тех же обстоятельствах. За исключением случаев, когда можно предоставить обоснованное и достаточное рациональное объяснение для обработки личной информации, приоритет всегда должен отдаваться защите интересов субъекта персональных данных.

Если персональные данные рассматриваются как «общественное благо» благодаря их социальной значимости, они одновременно сохраняют характер «частного блага» в силу своей привязки к индивидуальности человека. Рациональность использования и иных действий с персональными данными

[125] Чувство лишения неприкосновенности частной жизни — это новое понятие, которое в основном относится к восприятию человеком того, что он постоянно находится в невыгодном положении и не может сопротивляться во время обмена ресурсами конфиденциальности, что приводит к негативным эмоциям, таким как вторжение, тревога, гнев и даже субъективные чувства, которые проявляют склонность к тщетности. См.: *Ян Сиси, Ли Бенган.* Структурная депривация: логика формирования чувства лишения неприкосновенности частной жизни у алгоритмической аудитории // Журнал Шаньдунского педагогического университета. Общественные науки. 2023. № 6. С. 126.

может быть возложена на самого субъекта этих данных, однако без учета принципов человеческого достоинства и свободы информации такая рациональность становится абстрактной и теряет практическую применимость.

2) Справедливость распределения с учетом интересов, вытекающих из свободы информации. Защита персональных данных не только должна основываться на ценности человеческого достоинства, но и должна быть направлена на надлежащее распределение выгод между человеческим достоинством и свободой информации. Учет интересов свободы информации является основным требованием правовой системы защиты персональных данных для достижения справедливости при их распространении.

Ценность закона – это единство абсолютности и относительности. Среди них абсолютность ценности является критерием для измерения интересов, а относительность ценности делает необходимым равенство интересов. В настоящее время конфликт интересов в области защиты персональных данных в основном отражается в конфликте между желанием правительств, предприятий и т.д. чрезмерно получать и использовать персональные данные и ограничением передачи персональных информационных ресурсов. Даже сам субъект персональных данных иногда становится потребителем персональных информационных ресурсов.

Будь то правительство, коммерческая организация, некоммерческая организация или частное лицо, до тех пор, пока они выступают в роли потребителей персональных данных, у них есть определенная «концепция полезности», то есть они постоянно измеряют выгоды и потери при обмене личными информационными ресурсами для того, чтобы обеспечить максимальную степень их удовлетворенности.[126] В условиях парадигмы больших данных причина, по которой люди уделяют большое внимание добыче и использованию ценности персональных информационных ресурсов, заключается в том, что они могут принести конкретную пользу, такую как повышение

[126] *Ричард Познер.* Экономический анализ права. Перевод: *Цзян Чжаокан.* Пекин: Издательство китайской энциклопедии. 1997. С. 39.

социального благосостояния, эффективность государственного управления, корпоративная прибыль или преимущества социального общения.[127]

Персональные данные обладают бесспорным свойством полезности в современных условиях, но необходимо иметь более глубокое понимание «полезности» персональных информационных ресурсов, основанное на правилах в области конфиденциальности. Это в основном отражается в следующем:

Во-первых, полезность персональных данных воплощается в закономерности уменьшения предельного воздействия ценности персональной информации, что в основном выражается в незначительном снижении полезности для потребителей при использовании персональных данных по мере раскрытия скрытой ценности информации. Наиболее наглядный пример заключается в том, что нераскрытая информация при одних и тех же условиях более полезна, чем раскрытая информация, и чем больше потребляется аналогичной персональной информации, тем меньше увеличивается полезность для отдельных лиц.

Во-вторых, возникновение полезности ресурсов персональных данных может быть основано только на доброкачественном персональном информационном капитале. Являясь своего рода социальным капиталом, персональная информация будет постоянно изменяться в процессе производства, обмена, распределения и потребления. Следовательно, необходимо учитывать не только адекватность персонального информационного потенциала всего общества, но и структурную природу и устойчивость персональных данных.

Если субъект персональных данных не в состоянии адекватно оценить выгоду от удовлетворения личностных или иных интересов при обмене персональными данными, процесс производства такой информации может постепенно трансформироваться в феномен, аналогичный «вытеснению хороших денег плохими». Наконец, хотя объем персональных данных в обществе в целом по-прежнему огромен, он больше не отражает в полной мере индивидуальную волю (стремления, пожелания, требования и т.д.) субъекта персональной информации.

---

[127] *Ван Янь, Е Мин.* Конфликт и баланс между обменом персональными данными и защитой конфиденциальности в эпоху искусственного интеллекта // Введение в теорию. 2019. № 1. С. 99-106.

Прогнозирование и принятие решений на основе таких персональных информационных ресурсов, несомненно, станут катастрофой для всего общества.

В-третьих, при оценке полезности персональных данных необходимо учитывать баланс между выгодами и рисками. Таким образом, использование и защита персональных данных требуют поиска баланса между потенциальными выгодами и возможными рисками. При обработке персональной информации необходимо учитывать не только экономическую и социальную ценность данных, но и издержки, возникающие в связи с их сбором, передачей, хранением и обеспечением безопасности. В рамках защиты персональных данных ключевое значение имеет оценка того, насколько применяемые механизмы способны предотвращать злоупотребления и одновременно не препятствовать правомерному использованию информации. Для субъектов персональных данных это означает необходимость выбора таких способов распоряжения своими данными, которые позволяют минимизировать риски и сохранить ожидаемые преимущества от их передачи.

3) Поиск справедливого регулирования в рамках универсального правового порядка, основанного на балансе человеческого достоинства и свободы информации. Баланс интересов в сфере защиты персональных данных должен обеспечивать справедливый общественный контроль над обработкой персональной информации. Научно-технические инновации, социальные преобразования и укрепление верховенства права способствовали формированию правовых основ и защите интересов субъектов персональных данных, и формирование этого нового типа права будет способствовать дальнейшему развитию социальной практики и правовой системы. Можно сказать, что баланс интересов – это не только состояние порядка правовой справедливости, но и процесс реализации правовой справедливости.

Можно сказать, что концепция справедливости направлена на защиту права человека на свободу и справедливость в стремлении к общественному богатству

(экономическому, политическому и культурному)[128]. В современном рисковом обществе наиболее актуальной проблемой в сфере конфликта интересов при защите персональных данных является существование угрозы справедливому порядку. Справедливое и упорядоченное управление рисками, связанными с контролем личной информации, является не только неизбежным результатом процессов, происходящих в современном обществе,[129] но и способствует постоянному изменению и развитию методов контроля личной информации на основе стабильности и инноваций.

С одной стороны, риск нарушения справедливости и порядка при контроле личной информации отражается в структурных дисбалансах, то есть последовательное развитие информационно-коммуникационных технологий привело к структурным преобразованиям в сфере конфиденциальности. Наиболее примечательной особенностью является то, что персональные информационные ресурсы приобретают коммерческую ценность, а их незаконная обработка долгое время не изменялась, что привело к увеличению нарушений конфиденциальности со стороны отдельных лиц и сообщества в области неприкосновенности частной жизни.

С другой стороны, в связи с развитием больших данных, контроль за персональными данными ослабевает, причем независимо от оператора. В то же время, сдерживаемые такими факторами, как социальный статус, социальные ресурсы и экономическое развитие, субъекты персональных данных, находящиеся в центре традиционной системы защиты данных, постепенно исключаются из системы распределения конфиденциальных экономических и социальных благ, связанных с оборотом данных.

---

[128] По мнению Фридриха фон Хайека, универсальное правило для измерения «справедливости» должно быть найдено в «правовом порядке», то есть «закон относится ко всем одинаково»; с точки зрения Дворкина, равенство и свобода могут сосуществовать в гармонии, и равенство является более фундаментальной и стержневой ценностью; Ролз также считает, что справедливость — это первая добродетель социальной системы; справедливость – это всегда разновидность социальной справедливости, которая содержит принципы «свободы, равенства и дифференцированного отношения», чтобы наиболее обездоленные в обществе могли получить наибольшие выгоды. См.: *Фридрих фон Хайек.* Индивидуализм и экономический порядок. Перевод: Цзя Чжань и др. Пекин: Издательство Пекинского экономического института. 1989. С. 16; Рональд Дворкин. О правах всерьёз. Перевод: *Синь Чуньин, Ву Юйчжан.* Шанхай: Книжный магазин "Саньлянь". 2008. С. 139 362; Джон Ролс. Теория справедливости. Перевод: Хэ Хуайхун и др. Пекин: Издательство китайских общественных наук. 1988. С. 3, 60-62.

[129] *Ульрих Бек.* Общество риска. Перевод: *Хэ Бовэнь.* Нанкин: Издательство "Илинь". 2004. С.9.

Следовательно, правовая система защиты персональных данных должна быть такой социальной системой, которая удовлетворяет требованиям, необходимым для выживания цивилизованного общества, с наименьшими возможными затратами, а интересы к персональным данным признаются и гарантируются более всеобъемлющим и эффективным институциональным образом, таким образом, конфронтация и конфликт интересов между ними также все более и более полностью устраняются и разрешаются. В аспекте формальной справедливости, необходимо разработать ряд правовых систем и политик для признания, определения и защиты законных интересов, связанных с персональными данными, с тем чтобы гарантировать, что отдельные лица имеют разумные ожидания в отношении своей собственной информации, а также поддерживать, продвигать и наследовать порядок общественного контроля за обменом персональной информацией. Соответственно, материальная справедливость заключается в достижении единства законности и эффективности распределения прав, полномочий, обязанностей и ответственностей между членами общества.[130]

Таким образом, обеспечение безопасности персональных данных представляет собой совокупность правовых, организационных, технических и иных мер, направленных на установление состояния защищенности персональных данных, при котором отсутствует несанкционированный доступ к ним третьих лиц и не происходит их незаконная обработка. Меры защиты же предполагают меры, принимаемые в случае фактического нарушения прав субъектов персональных данных. Однако в отношении персональных данных имеется очень важная особенность. Персональные данные, несмотря на общий режим ограниченного доступа, в определённых случаях могут становиться открытыми, в частности по воле самого субъекта персональных данных. Вместе с тем факт раскрытия таких сведений не исключает необходимости их дальнейшей правовой и организационной защиты. Субъект персональных данных сохраняет

[130] *Янь Цуньшэн.* Исследование легитимности закона // Юридическая наука (Журнал Северо-Западного политико-юридического университета. 2002. № 3. С. 3-14.

возможность требовать соблюдения конфиденциальности в отношении уже раскрытой информации, а также принятия мер, предотвращающих её последующее неправомерное использование. Поэтому меры защиты в подобных случаях могут рассматриваться и как элементы обеспечения безопасности персональных данных, поскольку они направлены на поддержание более высокого уровня их защищённости. Следовательно, обеспечение безопасности персональных данных связано прежде всего с предупреждением нарушений прав субъектов персональных данных.[131] Меры защиты в этом случае имеют особое юридическое значение, поскольку их не следует полностью отождествлять с мерами безопасности. Вместе с тем они могут рассматриваться как неотъемлемая часть общего подхода к обеспечению безопасности персональных данных. Меры защиты персональных данных ликвидируют наступившие угрозы, например, в связи с утечкой персональных данных, но при этом выступают и мерами, направленным на дальнейшее обеспечение безопасности, то есть состояние защищенности прав субъекта персональных данных, предотвращая возможность их дальнейшего незаконной обработки, поскольку субъект персональных данных может быть заинтересован в дальнейшей конфиденциальности этих данных в отношении других лиц.

Правовое обеспечение безопасности персональных данных представляет собой комплексное сочетание принципов справедливости и обеспечения правопорядка, а также координации между «материальными интересами» и «институциональными интересами». С точки зрения эффективности, данная правовая система должна быть ориентирована на минимизацию затрат, связанных с обменом персональными данными, чтобы обеспечить социальную справедливость в отношении максимального увеличения объема персональных данных и запаса персональных данных выше минимального уровня. Хотя отдельные субъекты права предъявляют различные ценностные требования, по сути, они являются субъектами, защищающими свои собственные интересы,

---

[131] *Ван Гуанлун.* Механизм административного-правового регулирования защиты персональных данных в Китае: состояние, недостатки и путь решения. // Вестник Московского университета. 2024. Серия 11. Право. Том 65. № 4. С. 204-232.

обладающими ограниченными рациональными способностями и стремящимися к максимизации выгод. С точки зрения справедливости, правовое обеспечение безопасности персональных данных должно не только обеспечивать сбалансированную форму правовых благ в области персональной информации и поддерживать эффективный баланс между личными интересами, общественными интересами и интересами общества в целом, но и на основе человеческого достоинства и свободы создать материальную справедливость распределения результатов в рамках формальной справедливости.

Подводя итоги по параграфу и главе, можно сделать вывод, что человеческое достоинство и свобода информации формируют фундаментальную ценностную основу правового, в том числе публично-правового, обеспечения безопасности персональных данных. Это проявляется в том, что, с одной стороны, личная информация является непосредственным отражением достоинства и законных интересов субъекта информации, а с другой стороны, в соответствии с закрепленным в Китае принципом ценности свободы информации, обработка личной информации получает правовое обоснование. Показано, что такой ценностный дуализм находит конкретное выражение в законодательстве России и Китая, определяя различные подходы к построению баланса между обеспечением безопасности персональных данных и их обработкой. При этом правовое обеспечение безопасности персональных данных должно в первую очередь основываться на содержании человеческого достоинства, что проявляется в признании за субъектом персональных данных комплекса правомочий по контролю над своей личной информацией. Однако право на защиту персональных данных не признается абсолютным и должно рассматриваться в соответствии с его социальной функцией. Это означает, что оно должно быть сбалансировано с другими основными правами и законными интересами в соответствии с принципом пропорциональности, что находит свое отражение в установлении законодательных ограничений и исключений из общего режима защиты.

Сравнительный анализ российского и китайского законодательства в данной сфере позволяет не только выявить различные акценты в решении проблемы

баланса, но и определить взаимополезные элементы для совершенствования обеих систем с учётом их правовых традиций. Российский подход с его детализированной процедурной регламентацией оснований обработки данных может служить ориентиром для повышения формальной определённости и предсказуемости применения принципа соразмерности в правоприменении в Китае. В свою очередь, китайский опыт чёткого нормативного закрепления приоритета публичных интересов (национальной безопасности, общественного благополучия) в определённых законом случаях предлагает модель для более структурированного и транспарентного учёта этих интересов в российской правовой системе, особенно в контексте регулирования новых технологий. Таким образом, потенциал для взаимного совершенствования лежит не в заимствовании ценностных приоритетов, а в адаптации конкретных правовых механизмов и процедур: Россия может обогатиться более гибкими формулировками исключений в интересах общества, а Китай – более чёткими публично-правовыми мерами обеспечения безопасности в процессе обработки персональных данных и процессуальными гарантиями для защиты прав субъектов данных.

Установлено, что теоретической основой защиты персональных данных как в России, так и в Китае выступает механизм обеспечения баланса интересов. В Китае он концептуализирован в рамках «персональной кибернетики» и «социальной кибернетики», в России – в форме принципа баланса интересов личности, общества и государства, активно реализуемого в системе правового обеспечения информационной безопасности. Данный механизм направлен на определение, выявление и защиту прав и законных интересов граждан, связанных с персональными данными, с использованием комплекса правовых средств. В целях повышения эффективности данного механизма представляется необходимым дальнейшее развитие и конкретизация системы действующих принципов правового регулирования персональных данных в обоих государствах через призму задачи обеспечения баланса. Такой подход подразумевает, что баланс интересов всех участников отношений в сфере персональных данных должен выступать не только как отдельный принцип, но и как сквозная цель

применения других существующих принципов, таких как законность, справедливость, соразмерность, целевое ограничение и минимизация данных и другие. Это будет способствовать совершенствованию нормативных правовых актов, обеспечивая признание приоритета личностного достоинства, учёт общественных и государственных интересов, а также выявление и предотвращение потенциальных конфликтов между различными субъектами в процессе обеспечения безопасности и принятия мер защиты персональных данных.

Таким образом, научный и практический акцент смещается с провозглашения отдельного принципа баланса на анализ и оптимизацию взаимодействия конкретных правовых принципов и механизмов, которые фактически уже опосредуют достижение этого баланса в национальных механизмах обеспечения безопасности персональных данных.

# ГЛАВА II. ПУБЛИЧНО-ПРАВОВЫЕ МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В КИТАЕ И РОССИИ

## 2.1 Конституционные основы обеспечения безопасности персональных данных граждан в Китае и России

### 1. Конституционные меры обеспечения безопасности персональных данных в Китае

В условиях современного цифрового общества защита персональной информации приобрела разнообразные, сложные и предметно-ориентированные аспекты, что при обработке персональных данных сопровождается рисками. В контексте углубления построения цифрового правительства государственные органы становятся одним из важных субъектов обработки личной информации, и при этом возникают соответствующие риски посягательства со стороны публичной власти.

Растущий спрос граждан на публично-правовое обеспечение безопасности личной информации отражает ограниченность концепции о защите персональных данных, основанной в прошлом на частном праве. С этой целью необходимо изменить действующий в Китае приоритетный путь частноправовой защиты персональной информации, расширив сферу правовой защиты персональных данных посредством более активного внедрения публично-правовых мер обеспечения безопасности и мер защиты персональных данных, обеспечив тем самым права и законные интересы граждан, связанные с персональными данными. В том числе существует явная потребность в признании права на персональные данные в качестве основного конституционного права, чтобы соответствовать базовой логике и ценностной структуре системы нормативных правовых актов, которые регулируют сегодня отношения, связанные с персональными данными.

#### 1) Китайская модель по защите персональных данных на конституционно-правовом уровне

В Конституции Китая прямо не оговариваются соответствующие права в

отношении персональных данных. Когда законодатели принимают законы, на них неизбежно влияют политические, экономические, социальные и другие аспекты времени. В то же время невозможно предвидеть, какие новые права появятся в будущем обществе. В этой связи невозможно отрицать, что права и интересы, связанные с персональными данными, носят по своему значению характер конституционных основных прав несмотря на то, что они прямо не перечислены в нынешней Конституции КНР. Проанализировав систему гарантий прав, установленную Конституцией Китая, китайское академическое сообщество уже подтвердило, что определенные нормы Конституции могут охватывать защиту персональных данных. Все данные конституционные положения выступают фундаментальной конституционно-правовой мерой обеспечения безопасности персональных данных, составляя основу системы публично-правовых мер обеспечения безопасности персональных данных.

Статью 33 Конституции КНР,[132]как правило, называют «положением о правах человека», которое было включено в Конституцию при ее пересмотре в 2004 году. Указанная статья значительно расширила систему основных прав, закрепленную в Конституции Китая. Положение о правах человека воплощает «дух неполного перечисления» в нормативном смысле[133], так что те права гражданина, которые не перечислены в Конституции, но имеют характер основных прав и отражают ценность прав человека, могут быть защищены Конституцией. Это также обеспечивает предварительную основу для конституционной защиты персональных данных. Кроме того, статья 38 Конституции КНР закрепляет специальные нормы об охране достоинства человека.[134]

Статья 33 Конституции Китая, являющаяся началом второй главы «Основные права и обязанности граждан», представляет собой набор общих положений, которые играют руководящую роль во всей главе. Статья 38 также

---

[132] Статья 33 Конституции КНР гласит, что «Государство уважает и гарантирует права человека».

[133] *Линь Лайфань, Цзи Яньминь.* Значение защиты прав человека в качестве принципа // Исследование в области права и бизнеса. 2005. № 4. С. 66.

[134] Эта статья предусматривает, что «Достоинство граждан Китайской Народной Республики неприкосновенны. Запрещается каким бы то ни было способом подвергать граждан оскорблениям, клевете, ложным обвинениям и травле». См.: Конституция Китайской Народной Республики. URL: http://www.npc.gov.cn/zgrdw/npc/xinwen/2018-03/22/content_2052489.htm (дата обращения: 21.11.2024).

предусматривает защиту человеческого достоинства, что, можно сказать, является продолжением статьи 33. Человеческое достоинство — это универсальное, безусловное право, которым человек обладает по факту своего рождения[135]. Эта концепция была признана большинством государств и закреплена в их собственных конституциях. Юридическое понятие человеческого достоинства тесно взаимосвязано с концепцией прав человека, которая отражает объективные условия реализации потенциала, присущего каждому человеку как представителю вида, и подчеркивает универсальную ценность личности.[136] Китайские ученые в целом считают, что суть, корень и назначение основных прав заключаются в человеческом достоинстве[137]. Таким образом, основным правам, как правило, присуща ценность сохранения достоинства и уважения человеческой натуры.

Кроме того, статьи 39 и 40 Конституции КНР[138] устанавливают гарантии неприкосновенности жилища граждан, свободы и тайны переписки. По своему содержанию данные положения ориентированы на защиту частной жизни и связанных с ней правовых интересов личности. С учётом того, что конфиденциальность частной жизни может выступать одним из элементов права на персональные данные, указанные конституционные нормы нередко рассматриваются как дополнительное основание для отнесения права на персональные данные к числу фундаментальных прав человека.

Как справедливо указывает китайский исследователь Ван Кай, квалификация личной коммуникационной информации зависит от того, где именно она хранится. В случаях, когда записи переписки находятся у телекоммуникационной компании

---

[135] *Оботурова Н.С.* Концепт достоинства человека и его нравственно-правовое значение // Сетевой научно-практический журнал частного и публичного права. 2022. № 5 (20). С. 30.

[136] Как отметили российские авторы: «именно эта ценность делает каждое человеческое существо достойным … такого обращения, чтобы оно имело возможность реализовать свой потенциал и жить в мире с собой. Это субъективный коррелят объективной ценности человеческого существа». См.: *Кучуради И.* Понятия человеческого достоинства и прав человека // Вопросы философии. 2018. № 5. С. 49.

[137] *Ду Чэнмин.* Улучшение и реконструкция: Исследование основных прав в период социальных трансформаций. Пекин: Издательство Китайского политико-юридического университета. 2012. С. 20.

[138] Статья 39 Конституции КНР: «Жилище граждан Китайской Народной Республики неприкосновенно. Запрещается незаконный обыск или незаконное вторжение в жилище граждан»; статья 40 Конституции КНР: «Свобода и тайна переписки граждан Китайской Народной Республики охраняется законом. Никакие организации или отдельные лица ни под каким предлогом не могут препятствовать свободе и тайне переписки граждан, за исключением случаев, когда органы общественной безопасности или органы прокуратуры в порядке, установленном законом, осуществляют проверку переписки в интересах государственной безопасности или в целях расследования уголовного преступления».

или интернет-провайдера, они подлежат защите в рамках тайны переписки. Если же такие записи сохраняются на персональном устройстве лица, их правовая охрана может осуществляться через институт конфиденциальности частной жизни либо режим защиты персональных данных[139]. По мнению профессора Ду Цянцяна, записи телефонных разговоров, хотя и не относятся непосредственно к объектам защиты статьи 40 Конституции, могут подпадать под охрану конституционного права на неприкосновенность частной жизни. Это объясняется тем, что в отношении подобных коммуникаций у гражданина сохраняется разумное ожидание конфиденциальности[140]. Согласно последнему подходу, сведения, связанные с личной коммуникацией, подлежат разграничению в зависимости от того, какая модель конституционной защиты к ним применяется. Профессор Чжан Сян, в частности, прямо относит личную коммуникационную информацию к сфере защиты права на тайну переписки[141]. Вместе с тем, по мнению автора, право на личную коммуникацию и право на персональные данные не являются полностью изолированными правовыми категориями: между ними существует частичное пересечение, что требует комплексного подхода к их регулированию.

В действительности пересечение и возможная коллизия фундаментальных прав являются вполне характерными для конституционно-правового регулирования. Например, органы государственной безопасности могут незаконно проникать в жилище для ареста граждан, тем самым нарушая их право на личную свободу и неприкосновенность частной жизни, а также конституционное право на неприкосновенность жилища. Это проистекает из сложности социальных фактов и часто проявляется в смешанных формах, выходящих за рамки совокупности фактов, установленных нормами основных прав[142]. Некоторые ученые отмечают, что чем шире круг фактов, охватываемых нормами основных прав, тем выше

---

[139] *Ван Кай.* Защита основных прав в доступе к записям звонков (сообщений) // Политика и право. 2020. № 8. С. 111.

[140] *Ду Цянцян.* Доступ суда к записям телефонных разговоров не является проверкой связи в конституционном смысле // Правоведение. 2019. № 12. С. 85-86.

[141] *Чжан Сян.* Конституционное толкование права на переписку и рамки проверки: обсуждение с Ду Цянцяном, Ван Каем и Цинь Сяоцзянем // Журнал сравнительного правоведения. 2021. № 1. С. 41.

[142] *Линь Лайфань, Чжай Гоцян.* О конкуренции между основными правами // Юрист. 2006. № 5. С. 60.

вероятность конкуренции[143].

**2) Споры в сфере конституционно-правовой защиты персональных данных граждан в основном проявляются в следующих случаях.**

1. Спор о выборе прав в конституционно-правовом аспекте: концептуальное выражение основного права на защиту личную информации. Ряд китайских ученых выступают за придание персональной информации статуса фундаментального права, но конкретное концептуальное выражение этого права несколько отличается. При этом существуют две позиции: право на персональную информацию и право на самоопределение персональной информации.

Некоторые китайские ученые, с учетом опыта Германии,[144] попытались обосновать право личности на самоопределение персональной информации в Конституции Китая, подчеркнув контроль индивида над своей собственной информацией[145]. Однако эта позиция подверглась критике: одни ученые отметили, что защита личной информации не сосредоточена на самоопределении, а при индивидуальном контроле может легко вызвать чрезмерную защиту.[146] Другие считают, что право на информационное самоопределение является лишь концептуальным выражением вводящего в заблуждение представления о доминировании, которое не может быть приравнено к защите персональной информации[147].

Ученые, отстаивающие право на персональные данные, считают, что закрепление права на персональную информацию в Конституции Китая не означает, что оно является исключительным правом. Его основная функция заключается в установлении требований, посредством которых воплощается

---

[143] *Лю Цзяньлун.* О конкуренции между основными правами // Юрист. 2018. № 1. С. 33.

[144] Право на самоопределение персональных данных было закреплено в решении Федерального конституционного суда Германии по «Делу о переписи населения» в 1983 году, затем оно было продолжено в Законе о защите персональных данных, и в результате была создана система публичной правовой защиты персональных данных. См.: *Чжао Хун.* Текущая ситуация с защитой права на информационное самоопределение в нашей стране и перспективы развития законодательства в этой области // Обзор законодательства Китая. 2017. № 1. С. 151-152.

[145] *Яо Юэжун.* Подтверждение права на информационное самоопределение как одно из основных прав в нашей стране // Политика и право. 2012. № 4. С. 81.

[146] *Кун Сянвэнь.* Теоретическая критика и практические размышления о праве на самоопределение персональной информации: применение права принимать решения, предусмотренного статьей 44 Закона КНР о защите персональной информации // Исследование о модернизации системы верховенства права. 2022. № 4. С. 88.

[147] *Ян Фан.* Теория права на самоопределение персональной информации и ее просмотр и объект защиты Закона КНР о защите персональной информации // Журнал сравнительного правоведения. 2015. № 6. С. 33.

человеческое достоинство[148]. Фу Синьхуа подтвердил право на персональные данные, используя человеческое достоинство и автономию в качестве внутренних причин, а «общее благо» - в качестве внешних[149].

Полагаем, что в области конституционного права должна быть принята концепция права на персональные данные по следующим причинам: во-первых, право на самостоятельное определение личной информации подчеркивает слишком большой индивидуальный контроль над информацией, что, очевидно, несовместимо с особенностями передачи информации. Как отмечается исследователями, информационное самоопределение может быть лишь утопией, так как физические лица имеют определенное право на персональные данные, но они не во всяких случаях имеют право принимать окончательное решение в этом отношении[150]. Во-вторых, выражение концепции права на персональные данные характеризуется большей открытостью и соответствует особенностям развития человеческого достоинства. В контексте цифровой трансформации содержание человеческого достоинства постоянно расширяется: сфера права на персональные данные является гибкой, поэтому регулирование отношений в сфере персональных данных может развиваться под воздействием развития современных технологий.

2. Дискуссия о содержании статьи 38 Конституции КНР и его толковании. По вопросу о том, закрепляет ли эта статья одно из конкретных прав, или является общим базовым положением для развития системы прав, были проведены обширные дискуссии. Ученый Линь Лайфань разделил содержание этой статьи на две части, утверждая, что предыдущее предложение[151] выражает содержание, аналогичное основным конституционным ценностям, закрепленным в статье 1 Основного закона Германии «защита человеческого достоинства»[152]; последнее

---

[148] *Чжу Чжэнь.* Модель защиты прав: общественный характер и права в области защиты личной информации // Глобальный юридический обзор. 2022. № 1. С. 31.

[149] См.: *Фу Синьхуа.* Подтверждение права на персональную информацию // Правовая система и социальное развитие. 2021. № 5. С. 123-140.

[150] *Veil W.* The GDPR: The Emperor's New Clothes-On the Structural Shortcomings of Both the Old and the New Data Protection Law[J]. Neue Zeitschrift für Verwaltungsrecht, 2018, 10(2018): 686.

[151] То есть «Достоинство граждан Китайской Народной Республики неприкосновенны».

[152] Статья 1 (*«Человеческое достоинство неприкосновенно»*) — это самый важный раздел Основного Закона Германии (Grundgesetz). Она распространяется на все остальные основные права. В ней говорится о том, что

предложение[153] выражает содержание конкретных прав, которое эквивалентно личностному праву в конституции разных государств.[154] Оно может быть расширено и истолковано таким образом, чтобы включать в себя многие права, которые не указаны в Конституции, такие как права на жизнь, здоровье, портрет и т.д. Более того, даже некоторые новые права могут быть включены в эту группу исходя из расширительного толкования, например, экологические права и право на брачную автономию[155].

Однако некоторые ученые придерживаются альтернативной точки зрения. Так, профессор Се Либинь подчеркивает, что статья 38 Конституции КНР, регламентирующая одно из фундаментальных конституционных прав, не может рассматриваться как конституционный принцип ввиду своей специфической функциональной направленности.[156]

В условиях активного использования киберпространства сети Интернет персональные данные затрагивают все аспекты личной жизни и имеют существенно важное значение для каждого индивида. Работа и жизнь каждого человека больше связаны не только с реальным поведением в офлайне, но и во многом зависят от соответствующей цифровой жизни и действий человека как цифровой личности. Поэтому большинство китайских ученых считают, что в современную эпоху посягательство на личную информацию означает посягательство на человеческое достоинство. То есть положение Конституции КНР о гарантии человеческого достоинства можно рассматривать как основу для защиты персональных данных в современную эпоху. Иными словами, человеческое достоинство, закрепленное в статье 38 Конституции КНР, больше подходит в качестве основы конституционных прав, чем в качестве конкретного

---

каждый человек имеет ценность, так как он - человек. И такая ценность называется "достоинство". Все люди одинаковы, поэтому достоинство каждого человека должно находиться под защитой. При этом возраст, материальное положение, гражданство и т. д. не имеют никакого значения. См.: Основному закону Германии (Grundgesetz). https://handbookgermany.de/ru/basic-law (дата обращения: 27.11.2024)).

[153] То есть «Запрещается каким бы то ни было способом подвергать граждан оскорблениям, клевете, ложным обвинениям и травле»

[154] *Лин Лайфань.* Человеческое достоинство и достоинство человеческой личности: обсуждение о методах толкования статьи 38 Конституции КНР // Чжэцзянские общественные науки. 2008. № 3. С. 51.

[155] *Линь Лайфань, Ло Чжэнъянь.* Права личности в конституции // Юрист. 2008. № 5. С. 60-66.

[156] *Се Либин.* Китайско-немецкое сравнение человеческого достоинства в конституции: дискуссия с профессором Линь Лайфанем // Политический и юридический форум. 2010. № 4. С. 53-67.

базового права[157].

3. Споры о правовой природе права на персональные данные в Конституции КНР. В Законе КНР о защите персональной информации четко указано, что его законодательная основа исходит из Конституции КНР, что и разъясняет атрибуты права на персональные данные в качестве основного права[158], но в научных кругах все еще ведется дискуссия о месте права на персональные данные в системе конституционных прав Китая. В основном она включает в себя следующие две позиции：

а) Право на персональные данные входит в сферу существующих конституционных основных прав, а не является самостоятельным основным правом. Одни учёные рассматривают право на персональные данные как «комплекс основных прав». Научное обоснование атрибутов этого права, носящего характер «основных прав», может быть получено через толкование норм, касающихся права на неприкосновенность частной переписки и человеческого достоинства, закреплённых в положениях о правах человека.[159]

Другие подчеркнули, что права и интересы, связанные с персональными данными и регулируемые Законом КНР о ПДн, производны от основных прав, однако они не обладают характеристиками самостоятельных объектных интересов.[160] Права и интересы, касающиеся персональных данных, включают такие элементы публичного права, как человеческое достоинство, свобода и конфиденциальность коммуникации.[161] Право на коммуникацию как основное право может охватывать содержание права на персональные данные[162].

б) Право на персональные данные следует рассматривать как

---

[157] *Хань Дэцян.* О человеческом достоинстве: интерпретация теории человеческого достоинства с точки зрения права. Пекин: Юридическая пресса. 2009. С. 237.

[158] Согласно ст. 1 главы 1 Закона КНР о персональной информации «Настоящий Закон принят в соответствии с Конституцией …».

[159] Они считают, что защита права на персональные данные должна быть отнесена к различным положениям об основных правах в Конституции. См.: *Чжан Сян.* Конституционное подтверждение права на персональную информацию на основе размышления о теории разделения защиты и теории доминирования // Глобальный юридический обзор. 2022. № 1. С. 53-68.

[160] *Гао Фупин, Ли Цюньтао.* Новое позиционирование «прав и интересов в сфере персональной информации» в гражданском праве // Труды «Дунюэ». 2023. № 6. С. 166-176.

[161] *Чжан Синьбао.* О структуре прав и интересов в сфере персональной информации // Китайское и иностранное право. 2021. № 5. С. 1144-1166.

[162] *Чжан Янь, Сюй Цзясинь.* Переосмысление права на корреспонденцию в цифровую эпоху // Журнал «Чи-Лу». 2022. № 5. С. 94-105.

самостоятельный новый объект основных прав. Некоторые учёные полагают, что конституционная система основных прав предоставляет потенциальное правовое пространство для включения права на персональные данные. Однако, учитывая различия между объектом защиты личной информации и базовыми конституционными правами (такими как право на неприкосновенность частной жизни, право на переписку и защита репутации), право на персональные данные следует рассматривать как самостоятельное юридическое право, относящееся к категории права на человеческое достоинство.[163] При этом формулировка «в соответствии с Конституцией», закреплённая в Законе КНР о ПДн, повышает законодательный статус данного права, тем самым признавая персональные данные самостоятельным юридическим объектом и подчёркивая их особую правовую значимость.[164]

**2. Конституционные меры обеспечения безопасности персональных данных в России**

**1) Современное состояние конституционно-правового обеспечения безопасности персональных данных в России и существующие дискуссии по данному вопросу**

Основным нормативным правовым актом, обеспечивающим безопасность персональных данных граждан России, является Конституция Российской Федерации (далее – Конституция РФ). Данный акт лежит в основе всей системы публично-правовых мер обеспечения безопасности персональных данных. Несмотря на то, что Конституция РФ, как и Конституция КНР, прямо не содержит специальных положений о защите персональных данных, большинство российских исследователей сходятся во мнении, что её толкование должно осуществляться комплексно, с учетом конкретно-исторических условий. [165]

---

[163] *Хун Данна.* Место права на персональную информацию в системе конституционных прав нашей страны// Научный журнал о праве. 2024. № 3. С. 87

[164] *Тан Жуйфан.* Законодательная база, нормативное значение и системная структура защиты персональной информации: на основе положения законодательной базы Закона КНР о защите персональной информации // Хунаньские общественные науки. 2022. № 5. С. 109-117.

[165] Необходимость учета конкретно-исторических реалий применительно к истолкованию конституционных положений обусловлена тем фактом, что «конституция не может содержать универсальных правовых рецептов, рассчитанных на все времена… ее действие немыслимо без уточнения смысла ее положений, которые не могут восприниматься как неизменные». См.: *Арановский К., Князев С.* Роль конституции в политико-правовом обустройстве России:

Конституционно-правовые основы обеспечения безопасности персональных данных строятся на основе следующих положений Конституции Российской Федерации:

• части 1 статьи 23[166] в сочетании с частью 1 статьи 24[167], регламентирующей право на неприкосновенность частной жизни;

• части 2 статьи 23, устанавливающей право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений;

• статье 25, предусматривающей право на неприкосновенность жилища.

Следовательно, конституционно-правовые основы обеспечения безопасности персональных данных сформированы через систему конституционных прав, где объектом такой защиты выступают, в том числе, персональные данные. К числу таких прав относятся: право на неприкосновенность частной жизни; право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений; право на неприкосновенность жилища.

Следует подчеркнуть, что в современной российской юридической литературе право на неприкосновенность частной жизни традиционно интерпретируется как комплексное конституционное право, которое включает в себя такие составляющие, как право на неприкосновенность жилища и право на тайну переписки[168]. Данная правовая позиция представляется обоснованной, поскольку исторически указанные права были четко определены как инструменты защиты частной жизни личности.

Не отрицая неотъемлемой взаимосвязи между правом на неприкосновенность частной жизни и правами, закрепленными в статье 23 и части 2 статьи 25

---

исходные обстоятельства и современные ожидания // Сравнительное конституционное обозрение. 2013. № 3. С. 57; на изменчивость и подвижность смысла конституционных положений под влиянием объективных обстоятельств у казывает также Б. С. Эбзеев. См.: *Эбзеев Б. С.* Введение в Конституцию России. М.: Норма: ИНФРА-М, 2013. С. 10 4.

[166] Часть 1 ст. 23 Конституции РФ закрепляет право каждого на неприкосновенность частной жизни, личную и семейную тайну.

[167] Часть 1 ст. 24 Конституции РФ устанавливает прямой запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия.

[168] См., напр.: *Петрухин И. Л.* Личные тайны (человек и власть). М.: Институт государства и права РАН, 1998. С. 11–12; Конституция Российской Федерации. Доктринальный комментарий (постатейный) / рук. авт. кол. Ю. А. Дмитриев; науч. ред. Ю. И. Скуратов. 2-е изд., изм. и доп. М.: Статут, 2013. С. 103–104; Хужокова И. Право на неприкосновенность частной жизни в системе прав человека // Сравнительное конституционное обозрение. 2007. № 2. С. 32.

Конституции Российской Федерации, следует подчеркнуть, что право на тайну связи и право на неприкосновенность жилища представляют собой самостоятельные конституционные права [169], обладающие собственным содержанием [170] и выступающие специализированными институтами по отношению к общему праву на неприкосновенность частной жизни. Такой подход к пониманию взаимосвязи этих трех конституционных прав является основой для раскрытия их содержания с точки зрения того, в какой степени они охватывают защиту персональных данных[171].

Нормы ч. 1 ст. 23 с ч. 1 ст. 24 Конституции РФ рассматриваются в качестве основы конституционного права на неприкосновенность частной жизни[172]. Однако в данном контексте возникает вопрос о содержании понятия информации о частной жизни и его соотношении с категорией персональных данных. В российской конституционно-правовой доктрине по этому поводу сложились два основных подхода. Первый исходит из широкого понимания [173] информации о частной жизни, при котором она охватывает практически всеэлементы личной сферы гражданина, включая персональные данные. [174] Второй подход, напротив, предполагает более узкое толкование и проводит разграничение между сведениями, относящимися непосредственно к частной жизни, и данными, характеризующими иные стороны жизнедеятельности человека. Следует отметить, что Конституционный Суд Российской Федерации в своей практике

---

[169] Данный вывод, как представляется, находит подтверждение и в практике Конституционного Суда РФ, который рассматривает право на неприкосновенность частной жизни в качестве «фундаментального права», «в обеспечение» которого Конституция РФ закрепляет «иные личные права», в том числе право на тайну коммуникаций и право на неприкосновенность жилища. См.: Постановление Конституционного Суда РФ от 31 марта 2011 г. № 3-П // СЗ РФ. 2011. № 15. Ст. 2191.

[170] См.: *Романовский Г. Б.* Право на неприкосновенность частной жизни. М.: МЗ-Пресс, 2001. С. 34.

[171] *Проскурякова М.И.* Конституционно-правовые рамки защиты персональных данных в России // Вестник СПбГУ. Сер. 14. Право. 2016. Вып. 2. С. 13-14.

[172] В ряде решений Конституционный Суд РФ также указывал на ч. 1 ст. 23 и ч. 1 ст. 24 Конституции РФ как нормативную основу права на неприкосновенность частной жизни. См., напр.: Определение Конституционного Суда РФ от 29 января 2009 г. № 3-О-О (не опубликовано), Определение Конституционного Суда РФ от 29 сентября 2011 г. № 1063-О-О (не опубликовано). Здесь и далее ссылки на решения Конституционного Суда РФ приводятся по СПС «КонсультантПлюс» // www.consultant.ru (дата обращения: 13.03.2016).

[173] См.: *Авакьян С. А.* Конституционное право России. Учебный курс: Учеб. пособие: В 2 т. 5-е изд., перераб. и доп. М.: Норма, 2014. Т. 1. С. 670; Комментарий к Конституции Российской Федерации. / под ред. В. Д. Зорькина. 2-е изд. М.: Норма, 2011. С. 233.

[174] См.: *Проскурякова М.И.* Конституционно-правовые рамки защиты персональных данных в России // Вестник СПбГУ. Сер. 14. Право. 2016. Вып. 2. С. 12-27.

придерживается именно узкого подхода к пониманию данной категории. [175]

Соотношение категорий «информация о частной жизни» и «персональные данные» является непростым теоретико-правовым вопросом. Определение наиболее обоснованного подхода к их взаимосвязи требует специального анализа и учета различных правовых, социальных и технологических факторов. При этом данная проблема имеет не только теоретическое, но и практическое значение, поскольку от выбранной методологической основы во многом зависит корректное применение соответствующих правовых норм в правоприменительной практике. Кроме того, правильный теоретический подход к исследуемой проблеме поможет дать ответ на некоторые вопросы правоприменительной практики.

В российской юридической литературе существует три подхода к соотношению этих понятий, которые в основном проявляются в следующем:

а) Первая позиция утверждает, что понятие «информация о частной жизни» охватывает содержание «персональных данных», то есть взаимосвязь между ними характеризуется как отношение общего к частному. Данную точку зрения представляют такие учёные, как Э.А. Цадыкова[176], Н.И. Петрыкина[177]; К. В. Лапутько[178] и др.

б) Ученые, выступающие в поддержку второго подхода, полагают, что категория «персональные данные» является более широкой по сравнению с понятием «информация о частной жизни». [179]. Сторонниками этой позиции являются Е.В. Климович[180], Д.М. Ветров[181] и др.

---

[175] Например, в сферу частной жизни Конституционный Суд РФ не включает трудовые отношения, складывающиеся между работником и работодателем в рамках трудового договора, полагая, что они «носят общественный характер». См.: Определение Конституционного Суда РФ от 20 ноября 1998 г. № 157-О (не опубликовано).

[176] См.: *Цадыкова Э.А.* Гарантии охраны и защиты персональных данных человека и гражданина // Конституционное и муниципальное право. 2007. № 14.

[177] См.: *Петрыкина Н.И.* К вопросу о конфиденциальности персональных данных // Законы России: опыт, анализ, практика. 2007. № 6. С. 115.

[178] См.: *Лапутько К. В.* К вопросу о неприкосновенности частной жизни и защите данных // Право.by. 2022. № 1. С. 111.

[179] См.: *Важорова М.А.* Соотношение понятий «информация о частной жизни» и «персональные данные» // Вестник Саратовской государственной юридической академии. 2012. № 4 (87). С. 56-58.

[180] См.: *Климович Е.В.* О сущности понятия «персональные данные» как конфиденциальной информации особой категории // Международные юридические чтения: материалы ежегодной международной научно-практической конференции (14 апреля 2005 г.). Омск, 2005. Ч. 2. С. 27.

[181] См.: *Ветров Д.М.* Защита персональных данных и защита информации на предприятии. Некоторые спорные вопросы применения // Проблемы права. Челябинск, 2010. № 1. С. 119.

в) Согласно третьей позиции, категории «персональные данные» и «информация о частной жизни» не являются полностью идентичными, однако в определённых случаях их содержание может частично пересекаться[182].

Мы поддерживаем третью точку зрения, поскольку указанные категории различаются по своему содержанию и правовой природе. Персональные данные представляют собой любую информацию, прямо или косвенно относящуюся к определенному или идентифицируемому физическому лицу. К таким данным относятся адрес проживания, дата и место рождения, полное имя (фамилия, имя, отчество), информация о состоянии здоровья, семейном положении, имущественном состоянии, социальном статусе, личных взглядах и убеждениях, образовании, профессиональной деятельности, уровне доходов, а также сведения об интимной жизни[183]. Помимо этого, к персональным данным относятся уникальные идентификаторы, такие как идентификационный номер налогоплательщика, номер пенсионного удостоверения и другие аналогичные коды.

Отдельные ученые отмечают[184], что информация о частной жизни включает данные о конкретном человеке, не связанные с его профессиональной или общественной деятельностью. К таким сведениям относятся характеристики личности, внешность, состояние здоровья, финансовое положение, семейный статус, образ жизни, отдельные эпизоды биографии, а также взаимоотношения с родственниками, друзьями и знакомыми.[185]

Следовательно, два рассматриваемых понятия не совпадают по объёму[186]. Тем не менее, их содержание пересекается следующим образом: вся информация о частной жизни индивида персонифицирует его, отражая аспекты его

---

[182] См.: *Важорова М. А.* Соотношение понятий «Информация о частной жизни» и «Персональные данные» // Вестник СГЮА. 2012. №4 (87). С. 59.

[183] См.: *Добробаба М.А.* Понятие персональных данных: проблема правовой определенности // Вестник университета именно О.Е. Кутафина (МГЮА). 2023. №2. С.44.

[184] См.: *Пилипенко С.Г., Федосин С.А.* Указ. соч. С. 70.

[185] См.: *Малеина М.Н.* Личные неимущественные права граждан: понятие, осуществление, защита. М.: МЗ-Пресс, 2000. С. 153.

[186] Правильно отмечает *М. А. Важорова*, что понятия «информация о частной жизни» и «персональные данные» не тождественны, а «подход законодателя к правовому регулированию использования информации о частной жизни и персональных данных должен быть различным». См.: Важорова М. А. Соотношение понятий «Информация о частной жизни» и «Персональные данные» // Вестник СГЮА. 2012. №4 (87). С. 59.

деятельности в сфере частной жизни, и, таким образом, представляет собой сегмент категории персональных данных. Однако существуют значительные объемы персональных данных, которые, хотя и позволяют идентифицировать человека, не относятся к информации о частной жизни.[187] К примеру, к таким данным можно отнести фамилию, имя, отчество физического лица, информацию о профессиональной деятельности, участии в общественной жизни и т.д. Таким образом, даже упомянутые выше расширенные толкования понимания частной жизни не могут изменить того факта, что персональные данные являются независимым объектом, охраняемым Конституцией РФ.

Неслучайно, что конституционные акты целого ряда государств (в частности, Конституция Республики Беларусь[188], Конституция Венгерской Республики[189], Конституция Кыргызской Республики[190], Конституция Словакии[191], Конституция Республики Узбекистан[192],, Конституция Чехии[193] и других) закрепляют право на неприкосновенность частной жизни и право на защиту персональных данных.

---

[187] См.: *Пилипенко С.Г., Федосин С.А.* К вопросу о защите права на неприкосновенность частной жизни при обработке персональных данных // Актуальные проблемы современного государства и права: материалы Всероссийской научно-практической конференции (Саранск, 22–23 мая 2008 г.). М., 2009. С. 73.

[188] Часть 2 статьи 28 Конституции Республики Беларусь гласит: «… *Государство создает условия для защиты пер сональных данных и безопасности личности и общества при их использовании*». См.: Конституция Республики Бел арусь 1994 года (с изменениями и дополнениями, принятыми на республиканских референдумах 24 ноября 199 6 г., 17 октября 2004 г. и 27 февраля 2022 г.). Источник: https://pravo.by/pravovaya-informatsiya/normativnye-dokume nty/konstitutsiya-respubliki-belarus/ – Национальный правовой Интернет-портал Республики Беларусь (дата обращен ия 15.11.2024).

[189] Согласно части 1 статьи 59 Конституции Венгерской Республики, «В Венгерской Республике каждый обладает правом на доброе имя, неприкосновенность жилища, а также *правом на защиту* личной тайны и *персональных сведений*». См.: Конституция Венгерской Республики. https://constitutions.ru/?p=6509&ysclid=m8mdlz6p17315205031 (дата обращения: 24.03.2025).

[190] Часть 2 статьи 63 Конституции Кыргызской Республики гласит: «*Государство гарантирует каждому защиту персональных данных. Доступ к персональным данным граждан, их получение осуществляются только в предусмотренных законом случаях*». См.: Конституция Кыргызской Республики. URL: https://www.knu.kg/ky/ru/wp-content/uploads/sites/2/2024/02/const_kr.pdf (дата обращения 15.11.2024).

[191] Статья 19 Конституция Словакии гласит: «1. Каждый имеет право на уважение человеческого достоинства, личной чести, доброй репутации и на охрану имени. 2. Каждый имеет право на защиту от необоснованного вмешательства в частную и семейную жизнь. 3. *Каждый имеет право на защиту от необоснованного сбора или опубликования данных о своей личности либо иного злоупотребления ими».* См.: Конституция Словакии (Опубликовано 21 декабря 2008. Обновлено 4 января 2018. От 1 сентября 1992 года). https://constitutions.ru/?p=189&ysclid=m8mdkxylep428079660 (дата обращения: 24.03.2025).

[192] Согласно части 3 статьи 31 Конституции Узбекистана, «*Каждый имеет право на защиту своих персональных данных, а также требовать исправления недостоверных данных, уничтожения данных, собранных о нем незаконным путем или более не имеющих правовых оснований*». См.: Конституция Республики Узбекистана. URL: https://lex.uz/docs/6445147 (дата обращения 15.11.2024).

[193] Статья 10 Конституции Чехии гласит: «1. Каждый имеет право на уважение своего человеческого достоинства, личной чести, доброй репутации и на охрану имени. 2. Каждый имеет право на защиту от необоснованного вмешательства в частную и семейную жизнь. 3. *Каждый имеет право на защиту от необоснованного сбора или обнародования данных о своей личности либо иного злоупотребления ими».* См.: Конституция Чехии 1992 года с изм. 2009. URL: https://hrlib.kz/document/167704 (дата обращения: 24.03.2025).

Данное правовое регулирование обусловлено различиями в онтологической природе указанных категорий.

Следовательно, понятия «персональные данные» и «информация о частной жизни» не являются полностью идентичными, а характеризуются лишь частичным совпадением. Проведенное нами различие между указанными понятиями имеет как теоретическую, так и практическую значимость. Правовые нормы, регулирующие общественные отношения, должны учитывать специфику объектов этих отношений. Для повышения эффективности правового регулирования отношений, связанных с обработкой персональной информации, законодателям необходимо обратить внимание на обсуждаемую информацию (информацию о частной жизни или персональные данные). Иными словами, подход законодателей к правовому регулированию обеспечения безопасности информации о частной жизни и персональных данных должен быть различным.

**2) Проверка конституционности положений норм Закона РФ о ПДн**

Специфика системы правового регулирования персональных данных определяется интересами двух типов субъектов: один из них – это интересы субъекта персональных данных, а другой – интересы третьей стороны, обрабатывающей персональные данные. Правовые позиции Конституционного Суда Российской Федерации (далее – КС РФ) играют ключевую роль в решении указанных спорных ситуаций. Данные позиции также как и нормы Конституции РФ составляют сегодня гарантии, являющиеся конституционно-правовой мерой обеспечения безопасности персональных данных, а также основой для развития системы публично-правовых мер обеспечения безопасности персональных данных в России.

Следует подчеркнуть, что общественные отношения, регулируемые законодательством о персональных данных, хотя и относятся к информационной сфере, во многом развиваются на базе конституционно-правовых положений. Они тесно связаны с обеспечением права граждан на неприкосновенность частной жизни, а также смежных прав в контексте развития технологий автоматизированной обработки информации, тем самым подтверждая их

правозащитный характер.[194].

На практике был ряд споров по проверке конституционности положений норм Закон РФ о ПДн[195]. Так, по одному из споров о проверке конституционности Закона РФ о ПДн (п. 8 ч. 1 ст. 6) постановление КС РФ от 25.05.2021 № 22-П считается наиболее значимым правоприменительным актом[196]. С помощью этого специального дела КС РФ устранил значительную формальную неопределенность, которая долгое время сопровождала пункт 8 части 1 статьи 6 Закона РФ о ПДн, что оказало существенное влияние на последующую практику.[197] В другом споре о проверкЕ конституционности статьи 7 Закона РФ о ПДн заявительнице было отказано в предоставлении данных о третьих лицах, которые ранее были ее коллегами по учебному заведению. Гражданка посчитала, что норма ст. 7 Закона РФ о ПДн противоречит ч. 4 ст. 29 Конституции Российской Федерации, поскольку позволяет правоохранительным органам отказывать в предоставлении информации, необходимой для защиты нарушенных прав гражданина.[198]

Кроме того, из-за сложности соотношения между общими и специальными нормами, регулирующими обработку персональных данных, возникает множество коллизионных ситуаций между нормами Закона РФ о ПДн и нормами других отраслевых законов. В научных публикациях на соответствующую тему

---

[194] *Федосин А.С.* Защита конституционного права человека и гражданина на неприкосновенность частной жизни при автоматизированной обработке персональных данных в Российской Федерации: автореф. дис. … канд. юрид. наук. Саранск, 2009. С. 9.

[195] См.: Апелляционное определение Воронежского областного суда от 12.02.2019 г. по делу № 33–789; Апелляционное определение Воронежского областного суда от 30.05.2019 г. по делу № 33–3559; Апелляционное определение Воронежского областного суда от 12.03.2020 г. по делу № 33–1212; Апелляционное определение Воронежского областного суда от 05.08.2021 г. по делу № 33–4431/2021; Определение Воронежского областного суда от 22.07.2021 г. по делу № 33–4431/2021; Определение Четвертого кассационного суда общей юрисдикции от 25.11.2021 по делу № 88–20323/2021; Определение Четвертого кассационного суда общей юрисдикции от 08.06.2021 по делу № 88–13314/2021 и др.

[196] Здесь касается дела о проверке конституционности пункта 8 части 1 статьи 6 Федерального закона "О персональных данных" в связи с жалобой общества с ограниченной ответственностью "МедРейтинг".

[197] См. напр.: Определение Четвертого кассационного суда общей юрисдикции от 25.11.2021 по делу № 88–20323/2021; Определение Четвертого кассационного суда общей юрисдикции от 08.06.2021 по делу № 88–13314/2021.

[198] Конституционный Суд РФ решил, что норма Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» "О персональных данных", согласно которой операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, не противоречит Конституции РФ. Иными словами, Закон о защите персональных граждан не противоречит Конституции РФ. Текст скопирован с сайта ППТ: URL: https://ppt.ru/news/138028?ysclid=lqub73ookw38252577 (дата обращения: 15.11.2024).

отмечается, что одним из главных недостатков Закона РФ о ПДн является отсутствие четких критериев отнесения определенной информации к персональным данным, в результате чего одни и те же данные часто могут быть отнесены к разным видам информации с ограниченным доступом.[199]. Среди различных сфер оборота персональных данных, которые стали предметом рассмотрения в КС РФ, наиболее часто рассматриваемой сферой, было предоставление государственных и муниципальных услуг[200], включая спор о видеозаписи в кабинетах учреждений здравоохранения[201] и спор об ограничении процессуальных и профессиональных прав на истребование информации нормами Закона РФ о ПДн[202].

Анализ решений, принятых по этим спорам, показывает, что правовые позиции КС РФ в сфере персональных данных отражают стремление разрешить конкретную спорную ситуацию с точки зрения обеспечения баланса интересов субъекта персональных данных и интересов других лиц, сведения о которых содержатся в истребуемых им документах[203]. Почти все вышеперечисленные спорные ситуации свидетельствовали о конфликте частных и общественных интересов. Из практики конституционного судопроизводства в сфере персональных данных следует, что по своей природе споры носят в первую

---

[199] См.: *Кучеренко А.В.* Правовое регулирование персональных данных в Российской Федерации: автореф. дис. … канд. юрид. наук. Челябинск, 2010. С. 8.

[200] См.: *Соколова О.С.* Правовые позиции Конституционного Суда Российской Федерации в сфере персональных данных // Современное право. 2015. №10. С. 88-93.

[201] См.: Об отказе в принятии к рассмотрению жалобы гражданина Скипакевича Игоря Самуиловича на нарушение его конституционных прав пунктом 10 части 4 статьи 13, пунктом 5 статьи 78, статьями 87 и 90 Федерального закона «Об основах охраны здоровья граждан в Российской Федерации»: определение КС РФ от 24.09.2013 № 1333-О // Собрание законодательства РФ. 2011. №48. Ст. 6724.; Об отказе в принятии к рассмотрению жалобы гражданина Кудрякова Антона Васильевича на нарушение его конституционных прав положением части 1 статьи 25.1 Кодекса Российской Федерации об административных правонарушениях: определение КС РФ от 16.07.2013 № 1217-О // Доступ из СПС «КонсультантПлюс».

[202] См.: Об отказе в принятии к рассмотрению жалобы гражданина Глушкова Николая Петровича на нарушение его конституционных прав статьями 3, 5, 6 и 9 Федерального закона «Об информации, информационных технологиях и о защите информации» и статьями 8 и 9 Федерального закона «О персональных данных»: определение КС РФ от 29.01.2009 № 3-О-О // Доступ из СПС «КонсультантПлюс»; Об отказе в принятии к рассмотрению жалобы гражданина Багадурова Магомеда Магомедовича на нарушение его конституционных прав подпунктом 1 пункта 3 статьи 6 Федерального закона «Об адвокатской деятельности и адвокатуре в Российской Федерации», статьей 10 Федерального закона «О персональных данных» и частью второй статьи 57 Гражданского процессуального кодекса Российской Федерации: определение КС РФ от 29.09.2011 № 1063-О-О // Доступ из СПС «КонсультантПлюс».

[203] Об отказе в принятии к рассмотрению жалобы гражданина Солобуты Сергея Геннадьевича на нарушение его конституционных прав частью 2 статьи 9 Федерального закона «Об информации, информационных технологиях и о защите информации», статьей 7 и частью 1 статьи 19 Федерального закона «О персональных данных»: определение КС РФ от 23.12.2014 № 2941-О // Доступ из СПС «КонсультантПлюс».

очередь административно-правовой характер и возникают в связи с обработкой персональных данных в различных сферах государственного управления в процессе предоставления (или организации предоставления) услуг органами власти или подчиненными им учреждениями.[204]

Таким образом, на сегодняшний день было принято множество важных решений, в которых Конституционный суд Российской Федерации отказал в удовлетворении жалоб заявителей на неконституционность отдельных законодательных норм и не нашел оснований для признания оспариваемых законов не соответствующими Конституции Российской Федерации. В то же время содержание определений, трактующих оспариваемые нормы, чрезвычайно важно для правоприменительной практики в сфере обеспечения безопасности персональных данных. Конституционно-правовая природа отношений в сфере персональных данных определяет особую важность правовых позиций Конституционного Суда Российской Федерации в этой сфере. Учет этих позиций позволяет не только улучшить правоприменительную практику, но и определить направления совершенствования законодательства в сфере персональных данных.

## 2.2 Особенности административно-правового обеспечения безопасности персональных данных в Китае и России

Защита персональных данных от несанкционированного доступа со стороны государственных органов и субъектов, осуществляющих обработку данных, представляет собой одно из ключевых направлений в рамках публично-правового обеспечения безопасности персональных данных. Следует отметить, что автоматизированная обработка персональных данных различными операторами является объектом государственного контроля, что во многом способствует формированию общественного консенсуса относительно баланса между защитой данных и общественными интересами.[205]

**1. Административно-правовое обеспечение безопасности персональных**

---

[204] *Соколова О.С.* Правовые позиции Конституционного Суда Российской Федерации в сфере персональных данных // Современное право. 2015. №10. С. 88-93.

[205] *Ван Гуанлун.* Административно-правовая защита персональной информации в Китае: недостатки и путь решения // Вестник Университета имени О.Е. Кутафина (МГЮА). 2024. № 10. С. 189-197.

**данных в Китае**

**1) Административно-правовые меры обеспечения безопасности персональных данных в Китае**

Система административно-правового обеспечения безопасности персональных данных Китая, основанная на Конституции КНР, включает законы КНР[206], постановления административных регламентов Государственного совета КНР и иные нормативно-правовые акты.

Среди законов необходимо выделить следующие: Закон КНР о защите персональной информации (далее – Закон КНР о ПДн)[207]; Закон КНР об административном лицензировании[208]; Закон КНР о наказаниях за нарушение общественного порядка[209]; Закон КНР об административном пересмотре[210]; Закон Китая о кибербезопасности[211]; Закон КНР об административных наказаниях[212]; Закон КНР об аудите[213]; Закон КНР о безопасности данных[214]. Закон КНР о социальном страховании[215].

Среди административных регламентов необходимо выделить следующие:

---

[206] *Ван Гуанлун.* Механизм административно-правового регулирования защиты персональных данных в Китае: состояние, недостатки и путь решения. // Вестник Московского университета. 2024. Серия 11. Право. Том 65. № 4. С. 204-232.

[207] Этот закон в качестве специального законодательного акта устраняет пробелы в законодательстве Китая в области защиты персональных данных. В законе устанавливает общие правила обработки личной информации, права, которыми пользуется субъект информации, и обязанности обработчика информации в целях обеспечения прав на личную информацию и регулирования ее обработки. См.: Закон КНР о защите персональной информации. URL: http://www.npc.gov.cn/npc/c2/c30834/202108/t20210820_313088.html (дата обращения: 06.09.2025).

[208] См.: Закон КНР об административном лицензировании. URL: http://www.npc.gov.cn/npc/c2/c30834/201906/t20190608_298033.html (дата обращения: 06.01.2026).

[209] Закон КНР о наказаниях за нарушение общественного порядка. URL: https://m.lawtime.cn/faguizt/91.html (дата обращения: 06.01.2026).

[210] См.: Закон КНР об административном пересмотре. URL: https://www.gov.cn/yaowen/liebiao/202309/content_6901584.htm (дата обращения: 06.01.2026).

[211] См.: Закон КНР о кибербезопасности. Закон КНР о кибербезопасности вступил в силу 1 июня 2017 года. Всего 79 статей, который является первым всеобъемлющим законом Китая о кибербезопасности. Этот Закон применяется к владельцам, менеджерам и поставщикам сетевых услуг, которые создают, эксплуатируют, поддерживают и используют сети в Китае: URL: http://www.npc.gov.cn/zgrdw/npc/xinwen/2016-11/07/content_2001605.htm (дата обращения: 06.01.2026).

[212] См.: Закон КНР об административных наказаниях. URL: https://www.gov.cn/banshi/2005-08/21/content_25101.htm (дата обращения: 06.01.2026).

[213] См.: Закон КНР об аудите. URL: https://www.gov.cn/xinwen/2021-10/23/content_5644519.htm (дата обращения: 06.01.2024).

[214] См.: Закон КНР о безопасности данных. URL: http://www.npc.gov.cn/c2/c30834/202106/t20210610_311888.html (дата обращения: 06.01.2024).

[215] См.: Закона КНР о социальном страховании. URL: https://www.gov.cn/flfg/2010-10/28/content_1732964.htm (дата обращения: 06.01.2026).

Положение КНР об открытии государственной информации»[216]; Положение о национальной экономической переписи[217]; Положение об управлении отраслью кредитной отчетности[218]; Временные правила «О социальной помощи»[219]; Положение о защите несовершеннолетних в Интернете[220].

Кроме того, в Китае был также опубликованы ряд ведомственных нормативных актов в этом направлении, такие как Положение об управлении безопасностью персональной информации пользователей служб доставки[221] и др.[222]

**2) Правоприменительная практика в области обработки персональных данных в Китае**

Разработка и принятие Закона КНР о ПДн в 2021 году показало, что, с одной стороны, китайское правительство усилило административные меры по защите личной информации граждан, а с другой стороны, правонарушения в данной сфере стали приобретать все большую общественную вредность, а в некоторых случаях и общественную опасность.

В Китае органы общественной безопасности обладают двойными функциями: административной и судебной. Народные прокуратуры и народные суды являются судебными органами, которые специализируются на

---

[216] Положение КНР об открытии государственной информации было обнародовано Постановлением № 492 Государственного Совета Китайской Народной Республики от 5 апреля 2007 года, пересмотрено Постановлением № 711 Государственного Совета Китайской Народной Республики от 3 апреля 2019 года: URL: https://www.gov.cn/zhengce/content/2019-04/15/content_5382991.htm （Дата обращения: 12.12.2025）.

[217] Положение о национальной экономической переписи, обнародованное Постановлением Государственного Совета Китайской Народной Республики № 415 от 5 сентября 2004 года. 4 июля 2018 года на 15-м исполнительном заседании Государственного совета было принято «Решение Государственного совета о внесении изменений в Положение о национальной экономической переписи», и с 11 августа 2018 года было издано и приступило к реализации нового "Положения о национальной экономической переписи": URL: https://www.jj.gov.cn/art/2023/6/19/art_1229455069_1686988.html (дата обращения: 06.01.2026).

[218] Положение об управлении отраслью кредитной отчетности было принято на 228-м исполнительном заседании Государственного совета 26 декабря 2012 года и настоящим обнародовано и вступило в силу 15 марта 2013 года: URL: https://www.gov.cn/zwgk/2013-01/29/content_2322231.htm (дата обращения: 06.01.2026).

[219] Временные правила «О социальной помощи», опубликованные Постановлением Государственного совета КНР № 649 от 21 февраля 2014 г., вступившие в силу с 1 мая этого года: URL: https://www.gov.cn/flfg/2014-02/27/content_2624221.htm (дата обращения: 06.01.2026).

[220] Положение о защите несовершеннолетних в Интернете было принято на 15-м исполнительном заседании Государственного совета 20 сентября 2023 года и вступило в силу 1 января 2024 года: URL: https://www.gov.cn/zhengce/content/202310/content_6911288.htm (дата обращения: 15.01.2026).

[221] Положение об управлении безопасностью персональной информации пользователей служб доставки. URL: https://www.gov.cn/gongbao/content/2014/content_2711458.htm (дата обращения: 07.01.2026).

[222] Например, Положение о защите персональной информации детей в Интернете. URL: https://www.gov.cn/xinwen/2019-08/23/content_5423865.htm (дата обращения: 07.01.2026).

осуществлении прокурорских и судебных полномочий. Путем сбора дел, связанных с безопасностью данных и защитой личной информации, опубликованных на таких веб-сайтах, как Сеть Китайская сеть судебных документов[223], Китайская прокурорская сеть 12309[224], Китайская сеть документов по надзору за рынком и административным наказаниям[225], Юридическая база данных Пекинского университета «Бэйда-Фабао»[226] и т.д., можно сделать вывод, что органы общественной безопасности, Государственная администрация по регулированию рынка Китая (State Administration for Market Regulation, SAMR), Государственная канцелярия интернет-информации КНР и другие судебные и органы исполнительной власти в период с 2021 по 2023 год рассмотрели в общей сложности 888 административных дел, связанных с личной информацией граждан (Приложение 3).

Из вышеупомянутых 888 административных дел, связанных с персональными данными, 2 были возбуждены в 2021 году, 420 – в 2022 году и 466 - в 2023 году. Статистика судебных разбирательств показывает, что с 2021 по 2023 год количество таких административных дел росло из года в год.

Следовательно, в Китае с развитием и совершенствованием системы публично-правовых гарантий обеспечения безопасности персональных данных физические лица, юридические лица и государственные учреждения, осуществляющие обработку персональных данных, всё чаще подвергаются более строгому правовому регулированию в отношении соблюдения требований к защите и обработке персональных данных.

На основе анализа применяемых конкретных видов наказаний за вышеупомянутые правонарушения можно сделать вывод, что в рассматриваемый период были зафиксированы следующие меры административного воздействия: предупреждение или уведомление о критике (756), наложение штрафов, конфискация незаконно полученных доходов или изъятие незаконного имущества (337), приостановление действия лицензий, снижение уровня квалификации или

[223] URL: https://wenshu.court.gov.cn/ (дата обращения: 30.06.2025).
[224] URL: https://www.12309.gov.cn/ (дата обращения: 30.06.2025).
[225] URL: https://cfws.samr.gov.cn/ (дата обращения: 30.06.2025).
[226] URL: https://www.pkulaw.com/law?isFromV5=1 (дата обращения: 30.06.2025).

аннулирование лицензий (24), ограничение производственной или коммерческой деятельности, выдача предписаний о временном прекращении производства или бизнеса, а также закрытие предприятий или ограничение участия в определённых хозяйственных операциях (2). В 41 случае применялись иные административные санкции, предусмотренные законодательством и нормативными актами (Приложение 4).

Анализ приведённых статистических данных показывает, что система административной ответственности за нарушения в сфере персональных данных в Китае формируется главным образом на основе трёх нормативных правовых актов: Закона КНР о персональных данных, Закона КНР о безопасности данных и Закона КНР о кибербезопасности. Среди положений указанных актов особое значение имеют статьи 66, 51 и 17 Закона КНР о персональных данных, статьи 45, 27 и 29 Закона КНР о безопасности данных, а также статьи 64, 22 и 41 Закона КНР о кибербезопасности [227] . Они образуют основную нормативную базу для квалификации административных правонарушений в рассматриваемой сфере и применения соответствующих мер ответственности (Приложение 5).

Хотя Закон КНР о персональных данных и иные нормативные акты формируют относительно комплексный механизм защиты прав и законных интересов субъектов персональных данных, правоприменительная практика показывает необходимость дальнейшего ужесточения мер реагирования на соответствующие правонарушения. Административные и судебные органы уже добились определённых результатов в этой сфере, однако проблема утечек персональной информации по-прежнему сохраняет системный характер. В связи с этим раскрытые дела следует рассматривать лишь как видимую часть более широкого массива административных правонарушений в сфере персональных данных. Проблему утечки информации, которая может быть воспринята общественностью, по-прежнему трудно устранить, и граждане продолжают выражать обеспокоенность по поводу обеспечения безопасности своих

[227] *Ван Гуанлун.* Административно-правовые меры по обеспечению безопасности персональных данных при раскрытии информации правительством в Китае. // Вестник Санкт-Петербургского университета. Право. 2024. № 3. С. 815-834.

персональных данных. Согласно «Годовому отчету об исследовании «теневого» производства в Интернете за 2023 год», опубликованному Threat Hunter, число людей, занятых в черно-сером производстве в Интернете, продолжило расти в 2023 году, и их число достигло 5,871 миллиона, что на 141% больше, чем в предыдущем году; в 2023 году персональные данные по-прежнему оставались также основным типом утечки данных, составляющим более 90%[228].

В 2024 году инциденты с утечкой данных в Китае по-прежнему были частыми, как показано на Диаграмме 4 ниже[229]. Утечка отраслевых данных в этом году в основном касалась финансового сектора (20%), Информационной индустрии в Интернет (19%), оптовой и розничной торговли (10%), партийной, правительственной, военной и социальной сфер (9%), спорта и индустрии развлечений (6%), здравоохранения (126 инцидентов; 4%), транспортной и складской отрасли (118; 4%), обрабатывающей промышленности (110; 4%), образования (105; 4%), строительства и недвижимости (2%) и т.д. Согласно «Отчету о ситуации с риском утечки данных за первое полугодие 2024 года», подготовленному Threat Hunter, в первой половине 2024 года банки стали отраслью с наибольшим количеством инцидентов (всего 2961 инцидент), связанных с утечкой данных. Причинами утечки банковских данных являются уязвимости системы, хакерские атаки, внутренние утечки персонала и проблемы с управлением безопасностью сторонних партнеров[230]. Утечка банковских данных приведет к утечке личной информации клиентов, поставит под угрозу безопасность неприкосновенности частной жизни, также может быть использована для совершения преступных действий, таких как финансовое мошенничество, что приведет к экономическим потерям банков и клиентов (Приложение 6). В 2025 году данные тенденции усилились.

Следует указать, что исследовательская группа по кибербезопасности

---

[228] Отчет о делах, рассмотренных правоохранительными и судебными органами, по обеспечению безопасности данных за 2021-2023 годы. URL: https://zhuanlan.zhihu.com/p/692832359?utm_id=0&sid_for_share=99125_3&utm_source=wechat_session&utm_medium=social&s_r=0 (дата обращения: 07.01.2026).

[229] Анализ четырех типичных инцидентов с утечкой данных в 2024 году. URL: https://mbd.baidu.com/newspage/data/dtlandingsuper?nid=dt_5506380453569484345 (дата обращения: 06.01.2025).

[230] Отчету о ситуации с риском утечки данных за первое полугодие 2024 года. URL: https://www.thepaper.cn/newsDetail_forward_27963751 (дата обращения: 06.01.2025).

Cybernews обнаружила крупномасштабную утечку персональных данных граждан Китая в ходе продолжающегося кибератакового расследования. Согласно отчету, опубликованному этой группой, организация, возможно, неправильно настроила экземпляр Elasticsearch (широко используемый инструмент для хранения и поиска данных), в результате чего в общедоступную сеть просочилось более 1,2 миллиарда записей о личной информации. Вызывает тревогу тот факт, что группа Cybernews заметила, что этот пакет собранных данных, которые, как полагают, были получены в результате многочисленных предыдущих утечек, быстро увеличился с момента загрузки первой записи до более чем 123 миллиона записей всего за одну неделю, что означает, что этот набор данных все еще обновляется и расширяется. Объем утечки данных может достигать 100 ГБ, и каждая запись охватывает как минимум один телефонный номер. Кроме того, может быть задействовано больше личных данных и ранее нераскрытых наборов информации. В число объектов, пострадавших в результате этого инцидента утечки данных, входят сотни миллионов граждан Китая. Открытые записи не совсем понятны, но спорадическое количество незашифрованной информации в экземплярах Elasticsearch вызывает достаточную тревогу. Исследовательская группа Cybernews выпустила предупреждение: «Накопление такого огромного количества персональных данных может свидетельствовать об их потенциальном злонамеренном использовании». Исследователи также считают, что множество дубликатов может быть сделано для того, чтобы упростить объединение всей просочившейся информации об одной цели, создавая, таким образом, более всеобъемлющую угрозу личной информации[231].

**3) Административно-правовое обеспечение безопасности персональных данных при открытии государственных данных в Китае.**

Персональные данные играют ключевую роль в сфере государственного управления. В условиях развития цифровых технологий применение технологий больших данных трансформировало традиционные методы сбора и обработки

[231] Cybernews раскрыла масштабную утечку данных, касающуюся более чем 1,2 миллиарда граждан Китая. URL: https://www.163.com/dy/article/J34TIHFE0511A5GF.html (дата обращения: 06.01.2025).

личной информации граждан государственными учреждениями, обеспечив более эффективное и масштабное получение данных о населении. Тем не менее, такие изменения породили значительные вызовы в области обеспечения безопасности персональных данных граждан в рамках государственной системы открытых данных[232]. В современном Китае правовое регулирование в сфере раскрытия государственных данных основывается на комплексной системе нормативных правовых актов, включающей национальную политику, законодательство и другие нормативные документы различных уровней.

Национальные политики:

• Программа действий по содействию развитию больших данных[233];

• Главные тезисы 13-го пятилетнего плана социально-экономического развития Китайской Народной Республики[234];

• Постановление ЦК КПК по некоторым важным вопросам о сохранении и совершенствовании социалистического строя с китайской спецификой, стимулировании модернизации системы и потенциала государственного управления[235];

• План реализации построения правительства в условиях верховенства закона (2021-2025 годы)[236].

---

[232] *Ван Гуанлун.* Административно-правовые меры по обеспечению безопасности персональных данных при раскрытии информации правительством в Китае. // Вестник Санкт-Петербургского университета. Право. 2024. № 3. С. 815-834.

[233] В «Программе действий по содействию развитию больших данных», принятой Государственным советом КНР в 2015 году, было четко указано, что «при условии укрепления безопасности и защиты частной жизни в соответствии с законом неуклонно содействовать открытию публичных ресурсов данных». М.: Программа действий по содействию развитию больших данных. Пекин: Народное издательство, 2015. С. 9.

[234] В 2016 году Государственный совет КНР опубликовал «Главные тезисы 13-го пятилетнего плана социально-экономического развития Китайской Народной Республики», охватывающие период с 2016 по 2020 годы, в которых говорится о необходимости "разработки перечня совместного использования и открытия государственных данных и содействия открытию ресурсов данных для общества в соответствии с законом". См.: Программа 13-го пятилетнего плана социально-экономического развития Китайской Народной республики. Пекин: Народное издательство, 2016. С. 63.

[235] В «Постановлении ЦК КПК по некоторым важным вопросам о сохранении и совершенствовании социалистического строя с китайской спецификой, стимулировании модернизации системы и потенциала государственного управления», одобренном на 4-м пленуме ЦК КПК 19-го созыва, который с 28 по 31 октября проходил в Пекине, предлагается «содействовать созданию цифрового правительства и укреплять упорядоченный обмен данными». См.: Постановление ЦК КПК по некоторым важным вопросам о сохранении и совершенствовании социалистического строя с китайской спецификой, стимулировании модернизации системы и потенциала государственного управления. Пекин: Народное издательство, 2019. С. 18.

[236] В 2021 году Центральный комитет Коммунистической партии Китая и Государственный совет опубликовали «План реализации построения правительства в условиях верховенства закона (2021-2025 годы)», подчеркнув важность расширения исследований правовой системы в смежных областях, таких как цифровая экономика. См.:

Вышеупомянутые соответствующие документы на национальном уровне не только служат руководством для правительственных органов на всех уровнях в отношении дальнейшего устойчивого обеспечения открытия данных, но и демонстрирует, что открытое использование государственных общедоступных данных имеет огромное значение[237] для всестороннего развития во всех отраслях государства.

Национальные нормативные правовые акты[238]:

• Положение КНР об открытии государственной информации[239].

• Положение КНР о защите персональной информации пользователей телекоммуникаций и Интернета[240];

• Решение ПК ВСНП об усилении защиты онлайн-информации[241].

Так, на национальном уровне конкретный закон, регулирующий открытие государственных данных, в настоящее время в Китае еще не имеется. Нормативной основой в этом аспекте является Положение КНР об открытии государственной информации (далее именуемое «Положение») [242] . Однако содержание этого нормативного документа является относительно поверхностным

---

План реализации построения правительства в условиях верховенства закона (2021-2025 годы). URL: https://www.chinacourt.org/article/detail/2021/12/id/6460477.shtml (дата обращения: 14.12.2024).

[237] *Ван Гуанлун.* Административно-правовые меры по обеспечению безопасности персональных данных при раскрытии информации правительством в Китае. // Вестник Санкт-Петербургского университета. Право. 2024. № 3. С. 815-834.

[238] В настоящее время большинство законов и подзаконных актов Китая в области административного права содержат соответствующие положения о защите персональной информации. Кроме вышеупомянутых таких законов, как Закон КНР о защите персональной информации, Закон КНР о безопасности данных, Закон КНР о кибербезопасности и Закон КНР об административном пересмотре, включаются другие нормативные акты на национальном уровне.

[239] Положение Китайской Народной Республики об открытии государственной информации было обнародовано Постановлением № 492 Государственного Совета Китайской Народной Республики от 5 апреля 2007 года, пересмотрено Постановлением № 711 Государственного Совета Китайской Народной Республики от 3 апреля 2019 года. В этом документе указывается, что в процессе раскрытия информации о государственных делах информация, связанная с неприкосновенностью частной жизни, не подлежат разглашению, а также содержатся соответствующие положения о праве граждан изменять неверную персональную информацию. URL: https://www.gov.cn/zhengce/content/2019-04/15/content_5382991.htm (дата обращения: 15.12.2024).

[240] См.: Положение о защите персональной информации пользователей телекоммуникаций и Интернета, принятое Указом № 24 Министерства промышленности и информационных технологий Китайской Народной Республики от 16 июля 2013 года и вступившее в силу с 1 сентября 2013 года. URL: https://www.gov.cn/zhengce/2022-08/23/content_5722717.htm (дата обращения: 15.12.2024).

[241] См.: Решение Постоянного комитета Всекитайского собрания народных представителей об усилении защиты онлайн-информации, принятое на 30-м заседании Постоянного комитета 11-го Всекитайского собрания народных представителей 28 декабря 2012 г. URL: https://www.gov.cn/jrzg/2012-12/28/content_2301231.htm (дата обращения: 15.12.2024).

[242] См.: Положение Китайской Народной Республики об открытии государственной информации». URL: https://www.gov.cn/zhengce/content/2019-04/15/content_5382991.htm (дата обращения: 15.12.2024).

и не очень оперативным.

Пример местных нормативных правовых актов[243].

· Временные меры по открытию общедоступных данных в Шанхае[244];

· Временные меры по открытию общедоступных данных в провинции Гуандун[245] и т.д.;

· Положение муниципального правительства Гуйяна об открытии и использовании данных[246];

· Положение правительства провинции Гуйчжоу об открытии и использовании данных[247];

· Временные меры по открытию общедоступных данных и управлению безопасностью в провинции Чжэцзян[248]; и др.

Эти местные нормативные правовые акты содержат более подробные нормы об открытии данных, которые используются для руководства соответствующей работой местных органов власти по раскрытию данных.

Согласно перечню правительственных услуг, опубликованных в 2020 году, уровень открытия информации значительно возрос. По данным исследования некоторых ученых, соответствующие департаменты Государственного совета и все опрошенные трехуровневые органы власти, как провинциальные,

---

[243] В соответствии с требованиями национальной политики в Китае, местные правительства приняли соответствующие нормативные акты, направленные на создание и совершенствование системы управления открытым использованием государственных данных.

[244] Временные меры по открытию общедоступных данных в Шанхае, обнародованные Распоряжением № 21 Муниципального народного правительства Шанхая от 29 августа 2019 года, вступившие в силу с 1 октября 2019 года. URL: https://www.shanghai.gov.cn/nw45024/20200824/0001-45024_62638.html (дата обращения: 20.12.2024).

[245] Временные меры по открытию общедоступных данных в провинции Гуандун, обнародованные Распоряжением № 290 Народного правительства провинции Гуандун от 18 октября 2021 года, вступившие в силу с 25 ноября 2021 года. URL: https://www.gd.gov.cn/xxts/content/post_3584934.html (дата обращения: 20.12.2024).

[246] Положение муниципального правительства Гуйяна об открытии и использовании данных, принятое на 48-м засе дании Постоянного комитета 13-го Собрания народных представителей города Гуйян 24 января 2017 года, одобрен ное 27-м заседанием Постоянного комитета 12-го Собрания народных представителей провинции Гуйчжоу 30 март а 2017 года. URL: https://www.guiyang.gov.cn/zwgk/zfxxgks/fdzdgknr/lzyj/dfxfg/202106/t20210610_68479511.html (дат а обращения: 15.12.2024).

[247] Положение правительства провинции Гуйчжоу об открытии и использовании данных, принятое на 19-м заседании Постоянного комитета 13-го Собрания народных представителей провинции Гуйчжоу 25 сентября 2020 года и вступившее в силу 1 декабря 2020 года. URL: https://dsj.guizhou.gov.cn/xwzx/snyw/202009/t20200928_63601143.html (дата обращения: 20.12.2024).

[248] Положение правительства провинции Гуйчжоу об открытости и использовании данных, опубликованное распоряжением № 381 Народного правительства провинции Чжэцзян от 12 июня 2020 года, вступившее в силу с 1 августа 2020 года. URL: https://www.zj.gov.cn/art/2021/12/21/art_1229604638_2382460.html (дата обращения: 20.12.2024).

муниципальные, уездные (районные), раскрыли перечень правительственных услуг. Большинство правительственных органов продемонстрировали «полный жизненный цикл» обслуживания, включая 26 провинциальных правительств, 42 более крупных муниципальных правительства и 125 уездных (окружных) правительств, что доля от общего числа правительств того же уровня составляет 83,87%, 85,71% и 100% соответственно.[249]

Кроме того, согласно Отчету об открытии данных местных органов власти Китая, опубликованному Университетом Фудань в 2022 году, по состоянию на октябрь 2022 года всего 208 провинциальных и муниципальных органов власти в Китае запустили платформы открытости государственных данных, включая 21 платформу провинциального уровня (включая провинции и автономные районы, исключая муниципалитеты, непосредственно подчиняющиеся Центральному правительству, и правительства Гонконга, Макао и Тайваня) и 187 городских платформ. По сравнению со второй половиной 2021 года было добавлено 15 новых местных платформ, в том числе 1 провинциальная платформа и 14 городских платформ, и общее количество платформ увеличилось примерно на 8%.[250]

Очевидно, что соответствующие меры китайского правительства по открытию информации услуг были значительно усовершенствованы, что сделало запрос и получение информации более удобными. Однако следует отметить, что открытие правительственных данных Китая все еще находится на начальном уровне развития и при их открытии имеет много недостатков в сфере обеспечения безопасности личной информации.

Хотя Закон КНР о ПДн закрепляет относительно достаточные правовые гарантии обеспечения безопасности персональных данных граждан, большая часть его положений относится к субъектам персональных данных или лицам, которые обрабатывают персональные данные в частном секторе, и в нем очень

---

[249] *Ши Яньцзюнь.* Реальная дилемма открытого использования правительственных данных в эпоху больших данных и пути к его правовому обеспечению // Журнал Пекинского университета почты и телекоммуникаций. Общественные науки. 2023. № 6. С. 78.

[250] *Ся Цзиньлай.* Принятие административных решений с использованием больших данных в соответствии с законом // Журнал сравнительного правоведения. 2023. № 3 С. 138.

мало норм о государственных органах как субъектах обработки персональных данных. Существование подобной ситуации отражает пренебрежение статусом государственного аппарата как субъекта обработки персональных данных, что, несомненно, окажет негативное влияние на применение соответствующих положений Закона КНР о ПДн на практике.[251]

В действительности граждане предоставляют свои персональные данные государственным административным органам посредством различных сценариев применения, которые, в свою очередь, собирают и используют эти данные для выполнения функций общественного управления. При этом государственные органы занимают доминирующее положение, в то время как субъекты персональных данных часто теряют эффективный контроль над своей личной информацией. В результате слишком много персональных данных оказывается в распоряжении правительства, и оно также имеет право открыть эти данные. Это чаще всего может привести к ряду негативных последствий. Так, обработка персональных данных органами власти разных уровней без каких-либо ограничений может привести к нарушениям прав граждан на персональные данные. Например, в списке субсидий на страхование по старости в сельской местности и субсидий для студентов с низким доходом, объявленных округом Хуанпэй города Ухань в первом и втором кварталах 2018 года, правительство не только объявило имена тех, кто получил субсидии и помощь, но и указало их номера удостоверения личности, номера мобильных телефонов и конкретные домашние адреса на открытом правительственном портале.[252] Очевидно, что такого рода раскрытие номеров удостоверения личности, номеров мобильных телефонов и конкретных домашних адресов на официальном правительственном веб-сайте нарушает безопасность персональных данных граждан. Цель раскрытия правительством информации состоит в том, чтобы облегчить осуществление контроля со стороны населения, а не в неизбирательном и произвольном

[251] *Пен Чунь.* На основании законности обработка персональных данных государственными органами // Журнал сравнительного правоведения. 2022. № 1 С. 162-165.
[252] *Ян Ипин, Чэнь Цзе.* Защита личной информации при раскрытии правительственной информации в эпоху больших данных // Журнал Пекинского промышленного профессионально-технического колледжа. 2022. № 1. С. 99-100.

раскрытии информации. Иначе это может нарушить права граждан на персональные данные.

По нашему мнению, в процессе открытия правительством информации следует проводить различие между обычной и чувствительной личной информацией. Чувствительная информация, такая как номер удостоверения личности, номер мобильного телефона и т.п., не должна публиковаться напрямую, а требуется специальная обработка для снижения чувствительности такого рода информации; в то время как тривиальная информация, такая как имя, приблизительный адрес (не слишком точный адрес) и т.д., может быть опубликована напрямую. На самом деле, во многих случаях из-за того, что правительство не проводит четкую классификацию личной информации, возникает проблема утечки личной информации.

Тот факт, что правительство обладает значительной свободой усмотрения в вопросах открытия государственных данных, может привести к несоответствиям в судебных решениях по аналогичным делам. Приведем следующий пример. В сентябре 2016 года заявители Лю Гуансен, Лю Шиган и Лю Цзюньин обратились в Народное правительство уезда Пуян провинции Хэнань с просьбой раскрыть перечень конкретных данных о распределении компенсаций и субсидий в связи с экспроприацией земли и сносом домов для всех жителей деревни Тиелу уезда Пуян. В «Ответе на заявление о раскрытии правительственной информации Лю Гуансена, Лю Цзюньина и Лю Шигана» (далее именуемом «Ответ»), вынесенном правительством уезда Пуян, говорилось: «Правительственная информация, запрошенная Лю Гуансеном, Лю Шиганом и Лю Цзюньин, входит в сферу частичного раскрытия. За исключением Лю Гуансена, Лю Цзюньин Шиганга и Лю Цзюньина, информация о деталях выплаты компенсаций и субсидий в связи с экспроприацией земли и сносом домов для остальных сельских жителей относится к сфере личной конфиденциальности либо раскрытие этой части правительственной информации может привести к неправомерному нарушению прав на личную конфиденциальность. В соответствии со статьями 14 и 22 Положения Китайской Народной Республики о раскрытии правительственной

информации (далее именуемого "Положение"), эта часть информации раскрываться не будет». Лю Гуансен и др. не были удовлетворены «Ответом», поэтому они подали административный иск. Народный суд города Пуян провинции Хэнань в первой инстанции поддержал решение правительства уезда Пуян, полагая, что иск этих трех человек не имеет юридической основы, и отклонил их иск.[253] Лю Гуансен и др. подали апелляцию в Высший народный суд провинции Хэнань, который постановил, что правительственная информация, о раскрытии которой ходатайствовали заявители, не относится к их производственным, жизненным и другим потребностям, также не соответствовала вышеупомянутым требованиям законодательства, поэтому отклонил апелляцию и подтвердил первоначальное решение.[254] Далее они подали заявление о пересмотре дела в Верховный народный суд, который постановил, что:

а）Административный орган не раскрывал правительственную информацию на том основании, что она «относится к личной конфиденциальности или раскрытие может привести к ненадлежащему нарушению прав на личную конфиденциальность». Суды первой и второй инстанции прямо отклонили иск на том основании, что заявленная правительственная информация «не относится к их производственным, жизненным и другим потребностям». Это противоречит положениям судебного толкования.

б) Когда речь заходит о конфиденциальной личной информации третьих лиц, "Положение" предусматривает процедуру запроса мнений в письменной форме. Однако, Народное правительство уезда Пуян на основании того, что это дело касалось неприкосновенности частной жизни, непосредственно приняло решение об отказе в раскрытии соответствующей информации без соблюдения указанной процедуры.

в) Экспроприация коллективной земли, о которой идет речь в этом деле, должна применяться к соответствующим положениям об экспроприации земли и

[253] Решение промежуточного народного суда города Пуян провинции Хэнань по административному делу № 190-09/2016. Дата обращения 15 ноября, 2024. https://wenshu.lawtime.cn/.
[254] Решение Высшего народного суда провинции Хэнань по административному делу № 2075/2017. Дата обращения 16 ноября, 2024. https://wenshu.lawtime.cn/.

жилья, находящихся в государственной собственности, то есть сведения о выплате компенсаций сельским жителям относятся к правительственной информации, которая должна быть раскрыта. Подводя итоги, Верховный народный суд постановил отменить административные решения Суда первой инстанции и Суда второй инстанции по данному делу и «Ответ» Народного правительства уезда Пуян провинции Хэнань об отказе в раскрытии правительственной информации, и обязал Народное правительство Уезда Пуян провинции Хэнань предоставить заявленную правительственную информацию заявителям Лю Гуансену и другим лицам в течение 15 рабочих дней после вступления решения в силу.[255]

Как видно из вышеприведенных случаев, отношение органов власти и народных судов различных уровней к моментам об открытии правительственной информации сильно отличается. Фактически, это прямо связано с неясным определением в «Положении» таких понятий, как: общественные интересы, права и интересы на персональные данные (личную информацию), права общественности знать и права на личную конфиденциальность.

Статья 15 «Положения» предусматривает, что если открытие личной информации причинит вред третьей стороне, административный орган не открывает ее, однако, если третья сторона согласна или административный орган считает, что нераскрытие соответствующей информации может оказать значительное влияние на общественные интересы, она должна быть раскрыта.

Таким образом, разрешение противоречия между общественными интересами и законными интересами отдельных лиц, правом общественности на информацию и правом личности на конфиденциальность стало одной из ключевых проблем в современной судебной практике Китая[256].

**2. Административно-правовое обеспечение безопасности персональных данных в России**

В Российской Федерации правовой основой по обеспечению безопасности

---

[255] Решение Верховного народного суда Китайской Народной Республики по административному делу № 180/2018. Дата обращения 16 ноября, 2024. https://wenshu.lawtime.cn/.

[256] *Ван Гуанлун.* Механизм административно-правового регулирования защиты персональных данных в Китае: состояние, недостатки и путь решения. // Вестник Московского университета. 2024. Серия 11. Право. Том 65. № 4. С. 204-232.

персональных данных являются Конституция РФ, ряд федеральных законов и подзаконных нормативных правовых актов.

**1) Меры обеспечения безопасности персональных данных в административном и информационном праве России**

Нормативная основа для решения вопросов, связанных с обеспечением безопасности персональных данных, является важной и основополагающей.[257] К наиболее важным нормативным правовым актам в этой сфере необходимо отнести следующие.

Федеральное законодательство: Федеральный закон № 152-ФЗ «О персональных данных» (далее – ФЗ о ПДн); Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; Федеральный закон № 40-ФЗ «О федеральной службе безопасности»; Федеральный закон № 126-ФЗ «О связи»; Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»; Федеральный закон № 5485-1 «О государственной тайне»; Федеральный закон № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»; Федеральный закон № 8-ФЗ «О Всероссийской переписки населения»; Федеральный закон № 125-ФЗ «Об архивном деле в Российской Федерации»; иные федеральные законы[258].

Подзаконные нормативные правовые акты: указы и распоряжения Президента РФ[259]; акты Правительства РФ[260]; нормативные правовые акты федеральных

---

[257] *Назаров Д.М.* Основы обеспечения безопасности персональных данных в организации: учеб. пособие / Д.М. Назаров, К.М. Саматов; М-во науки и высш. Образования Рос. Федерации, Урал. гос. экон. ун-т. Екатеринбург: Изд-во Урал. гос. экон. ун-та, 2019. С. 13-17.

[258] Часть норм, определяющих отдельные случаи регулирования обработки персональных данных, содержится в кодексах. Например, Кодекс РФ об административных правонарушения, Гражданский кодекс РФ, Семейный кодекс РФ, Трудовой кодекс РФ и др.

[259] Включаются Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»; Указ Президента РФ от 30 мая 2005 г. № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела» и др.

[260] Например, постановление Правительства РФ от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»; постановление Правительства РФ от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных» и др.

органов исполнительной власти[261]; акты органов местного самоуправления в пределах их полномочий.

Локальные нормативные акты[262]. Сфера персональных данных представляет собой одну из наиболее урегулированных с позиции локальных правовых актов. Анализ законодательства о персональных данных свидетельствует, что в отдельные периоды его развития в России применительно отдельных видов юридических лиц требовалось разрабатывать до 12 видов таких локальных актов, посвященных разных аспектам обеспечения безопасности персональных данных. Действующее законодательство о персональных данных значительно сократило данный перечень.

Формируется и система нормативных правовых актов в сфере контрольно-надзорной деятельности в сфере персональных данных: «Федеральный закон от 31.07.2020 № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации»; Постановление Правительства Российской Федерации от 29.06.2021 № 1046 «О федеральном государственном контроле (надзоре) за обработкой персональных данных» (вместе с «Положением о федеральном государственном контроле (надзоре) за обработкой персональных данных»); Постановление Правительства Российской Федерации от 10.03.2022 № 336 «Об особенностях организации и осуществления государственного контроля (надзора), муниципального контроля»; Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 15.11.2021 № 1187 «Об утверждении перечня индикаторов риска нарушения обязательных требований при осуществлении федерального государственного контроля (надзора) за обработкой персональных данных»; Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 10.12.2021 № 1331 «Об утверждении индикативных показателей для федерального государственного контроля (надзора) за обработкой персональных данных»; Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых

[261] Включая приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 20 июня 2012 г. № 621 «О Консультативном совете при уполномоченном органе по защите прав субъектов персональных данных» и др.

[262] Эти акты предусматривают порядок обработки персональных данных и их защиты в конкретной организации.

коммуникаций от 24.12.2021 № 253 «Об утверждении формы проверочного листа (списка контрольных вопросов, ответы на которые свидетельствуют о соблюдении или несоблюдении контролируемым лицом обязательных требований), применяемого при осуществлении федерального государственного контроля (надзора) за обработкой персональных данных Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций и ее территориальными органами"»[263].

Можно выделить следующие особенности публично-правового регулирования обеспечения безопасности персональных данных:

Во-первых, защита персональных данных в России регулируется целым рядом нормативных правовых актов различного уровня, наиболее важным из которых является ФЗ о ПДн. Таким образом, мы можем говорить о формирующейся системе, которая объединяется в рамках комплексного правового института правового регулирования персональных данных, являющимся важной частью подотрасли правового регулирования информационной безопасности в рамках комплексной отрасли информационного права. Основой данного комплексного института при этом являются нормы информационного законодательства.

Во-вторых, в последние годы в России наблюдается активное развитие публично-правового регулирования персональных данных. Это выражается как во внесении изменений в действующее законодательство, так и в принятии новых подзаконных актов, направленных на уточнение порядка обработки персональных данных и обеспечение конфиденциальности информации[264]. При этом следует подчеркнуть, что значительная часть рассматриваемых законодательных новелл имеет публично-правовой характер и направлена на усиление механизмов обеспечения безопасности персональных данных. Особое место среди них

[263] Контрольно-надзорная деятельность. URL: https://rkn.gov.ru/activity/personal-data/supervisory/ (дата обращения: 30.04.2026).

[264] К таким документам относится Федеральный закон «О персональных данных» от 27.07.2006 №152-ФЗ и федеральные законы, вносящие в него последующие изменения (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2011, № 31, ст. 4701; 2013, № 14, ст. 1651; № 51, ст. 6683; 2014, № 30, ст. 4243; 2016, № 27, ст. 4164; 2017, № 27, ст. 3945; № 31, ст. 4772; 2020, № 17, ст. 2701; 2021, № 1, ст. 54, 58; № 27, ст. 5159; 2022, № 29, ст. 5233; 2024, № 33 (часть I), ст. 4929; 2024, № 53 (Часть I), ст. 8529; 2025, № 9, ст. 85; 2025, № 21, ст. 2542; 2025, № 26 (часть I), ст. 3486) и др.

занимают меры, связанные с усилением административной ответственности за нарушение законодательства о персональных данных.[265] В России в последние годы наблюдается общемировая тенденция к усилению ответственности, что свидетельствует о повышении общественной значимости отношений, связанных с персональными данными, обусловленном значительными утечками персональных данных. Таким образом, Россия проводит активную политику по публично-правовой защите прав и законных интересов в сфере персональных данных, что свидетельствует о реализации целенаправленной государственной политики в данном вопросе.

В-третьих, для обеспечения информационной безопасности критической информационной инфраструктуры (далее – КИИ) государством был разработан целый ряд документов[266]. Следует отметить, что все критически важные информационные инфраструктуры должны быть подключены к государственной системе обнаружения, предотвращения и ликвидации последствий компьютерных атак (ГОСОПКА) с целью создания обмена информацией о кибератаках на информационные системы, нарушение или прекращение работы которых наступят очень серьёзные последствия. Более того, данные об инцидентах на значимых объектах КИИ автоматически передаются ГОСОПКУ[267]. Таким образом, законодательство о персональных данных России сегодня является также неотъемлемой частью системы правового обеспечения кибербезопасности России.

**2) Правоприменительная практика в области обработки персональных данных в России**

Уполномоченным органом по надзору и контролю за защитой прав субъектов персональных данных в Российской Федерации является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее – Роскомнадзор). В целях обеспечения соблюдения законодательства о

---

[265] *Ван Гуанлун.* Механизм административно-правового регулирования защиты персональных данных в Китае: состояние, недостатки и путь решения. // Вестник Московского университета. 2024. Серия 11. Право. Том 65. № 4. С. 204-232.

[266] Включая Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 187-ФЗ // Собрание законодательства РФ. 2017. № 31 (1 ч.). Ст. 4736 и др.

[267] Утечки данных 2022: статистика, штрафы и меры по снижению рисков. URL: https://infobezopasnost.ru/blog/articles/utechki-dannyh-2022-statistika-tendentsii-kiberbezopasnosti-i-mery-po-snizheniyu-riskov-vzloma/ (дата обращения: 30.12.2024).

персональных данных и регулирования процесса их обработки Роскомнадзор может применять меры воздействия к нарушителям. [268] Особенно следует подчеркнуть, что Роскомнадзор обладает полномочиями по привлечению к административной ответственности за нарушения законодательства в сфере персональных данных. Вынесенные решения могут быть обжалованы в судебном порядке, если заявитель считает их необоснованными или незаконными. Нарушения требований законодательства о персональных данных безусловно вынуждают заинтересованных лиц, чьи права нарушены, обращаться в Роскомнадзор и (или) в суд для защиты своих прав.[269]

Так, по данным Роскомнадзора, всего за 2021 год с жалобами на неправомерную обработку персональных данных в ведомство обратились более 38 тыс. человек. Большинство жалоб было направлено на работу интернет-сервисов, организаций из сферы Жилищно-коммунального хозяйства (ЖКХ) и финансов, а также коллекторских агентств. За этот год Роскомнадзор провел более 3,9 тыс. проверок, 80% из которых выявили нарушения в работе операторов персональных данных. После проведенных проверок в список нарушителей ФЗ о ПДн попали 93 интернет-ресурса и было составлено 220 протоколов о привлечении к административной ответственности.

В числе самых распространенных нарушений можно выделить: отсутствие ответственного за обработку и хранение персональных данных, внутреннего контроля и обеспечения необходимых мер безопасности персональных данных, а также правовых оснований для хранения и обработки персональных данных. Результатом таких нарушений являются регулярные утечки персональных данных

---

[268] *Жердина С.Ю., Двенадцатова Т.И.* Защита персональных данных: первые итоги и перспективы судебных дел // Акционерное общество. 2017. № 11. С. 73.

[269] По статистике из офиц. соц. сетей и представителей РКН: В 2022 году произошло около 150 крупных утечек персональных данных. Прошло 78 внеплановых проверок по фактам утечек, и в 87% случаев факты незаконного распространения личной информации подтвердились. В суд направили 66 протоколов об административных правонарушениях. По результатам рассмотрения суды назначили штрафы на общую сумму лишь около 1 млн рублей, а также вынесли 9 предупреждений. Порядка 40 крупных утечек персональных данных уже зафиксировано в России на апрель 2023 г. Сравнимые периоды: первое полугодие 2022 и 2023 гг. Источник: Отчёты. Результаты деятельности. Типовые нарушения, выявленные Управлением. URL: https://59.rkn.gov.ru/p20924/p20925/ (дата обращения: 30.12.2024).

граждан[270].

Из содержания отчета, подготовленного экспертами юридического отдела RTM Group, видно, что в последние годы количество операторов персональных данных (Реестр операторов персональных данных) увеличилось[271]. Основные нарушения, совершенные указанными операторами, схожи, что заключается в основном в следующих аспектах:

- непринятие оператором необходимых и достаточных мер для обеспечения исполнения обязательств, предусмотренных ФЗ о ПДн[272];

- отсутствие согласия субъекта персональных данных при обработке его персональных данных;

- неправомерная обработка персональных данных субъекта (в том числе специальных и биометрических персональных данных, а также персональных данных третьих лиц) в сети Интернет либо в общественных местах;

- отправка рекламных рассылок/звонков соответствующим лицам без правовых оснований обработки персональных данных;

- незаконная передача данных за рубеж.[273]

Так, соответствующая статистика[274] показывает, что в период с 01 января 2022 года по 01 июля 2022 года было опубликовано 4,855 тыс. судебных дел, связанных с обработкой персональных данных. За аналогичный период 2023 года было вынесено уже 5,875 тыс. судебных актов, что свидетельствует об увеличении количества судебных решений в категории персональных данных на 21%.

В частности, это касается нарушений в сфере работы с персональными данными в категории административных споров: 18% - за 7 месяцев 2022

---

[270] См.: 80% проверок Роскомнадзора в 2021 году выявили нарушения в сфере обработки персональных данных. URL: https://itprotect.ru/mediacenter/blog/80-proverok-roskomnadzora-v-2021-godu-vyyavili-narusheniya-v-sfere-obrabotki-personalnykh-dannykh/ (дата обращения: 30.12.2024).

[271] С 15 178 в конце первого полугодия 2022 года до 21 360 в конце первого полугодия 2023 года (на 41% больше). За полгода 2022 г. была внесена 631 запись в реестр, а за полгода 2023 г. уже 1152, то есть почти в 2 раза больше. Источник данных: Отчёты. Результаты деятельности. Типовые нарушения, выявленные Управлением. URL: https://59.rkn.gov.ru/p20924/p20925/ (дата обращения: 05.01.2025).

[272] Здесь касается проверки надлежащего субъекта, меры защиты персональных данных и т.д.

[273] См.: Обработка персональных данных в России: судебная практика и правовое регулирование. URL: https://rtmtech.ru/research/obrabotka-pdn-v-rossii/ (дата обращения: 30.12.2024).

[274] Обработка персональных данных в России: судебная практика и правовое регулирование. https://rtmtech.ru/research/obrabotka-pdn-v-rossii/ (дата обращения: 30.12.2024).

года, 10% - за 7 месяцев 2023 года.

Согласно данным «Лаборатории Касперского» за 2022 год, в открытый доступ были выложены более 2 миллиардов записей, содержащих персональные данные и иную конфиденциальную информацию, из которых 16% составляли украденные пароли пользователей. Было установлено, что 64% утечек данных произошли в результате атак на крупный бизнес. В разрезе сфер деятельности, наибольшее количество утечек в Российской Федерации за 2022 год пришлось на ритейлеров – 14%, а также на сервисы доставки – 34%. Необходимо отметить, что среди скомпрометированных данных содержались как личные сведения сотрудников организаций, так и их клиентов.[275]

В России существенно вырос спрос на скомпрометированные базы данных россиян, в которых может содержаться чувствительная информация о личной жизни человека: медицинских анализах, выданных займах и даже доставках продуктов. В 2021 году было зафиксировано лишь четыре крупных инцидента с персональными данными, когда в открытый доступ попало 2,7 млн. записей. В 2022 г. – более 140 случаев, когда утекло около 600 млн. записей о гражданах[276].

В 2023 году в России зафиксированы 656 киберинцидентов, связанных с утечкой персональных данных. При этом были похищены приблизительно 1,12 млрд. записей. Для сравнения, годом ранее число инцидентов равнялось 770, тогда как количество скомпрометированных записей составляло около 702 млн. В 2023-м подавляющее большинство утечек персональных данных в РФ произошло в результате кибератак – 82,7%. Еще 10,1% случаев связаны с умышленными действиями внутренних сотрудников предприятий, 1,2% – со случайными действиями работников[277].

По информации InfoWatch, общее количество зарегистрированных

---

[275] Утечки данных 2022: статистика, штрафы и меры по снижению рисков. URL: https://infobezopasnost.ru/blog/articles/utechki-dannyh-2022-statistika-tendentsii-kiberbezopasnosti-i-mery-po-snizheniyu-riskov-vzloma/ (дата обращения: 30.12.2024).

[276] Личное делят: в РФ в 40 раз выросло количество утечек персональных данных. URL: https://iz.ru/1554402/alena-nefedova/lichnoe-deliat-v-rf-v-40-raz-vyroslo-kolichestvo-utechek-personalnykh-dannykh (дата обращения: 30.12.2024).

[277] Информация о утечке персональных данных за 2023 год исходит из статистике на сайте «Лаборатория Касперского Kaspersky». URL: https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:%D0%9B%D0%B0%D0%B1%D0%BE%D1%80%D0%B0%D1%82%D0%BE%D1%80%D0%B8%D1%8F_%D0%9A%D0%B0%D1%81%D0%BF%D0%B5%D1%80%D1%81%D0%BA%D0%BE%D0%B3%D0%BE_(Kaspersky) (дата обращения: 30.12.2024).

инцидентов в 2024 году составило 415, что на 10,1% больше, чем в первой половине 2023 года (377 утечек). По словам эксперта, количество утечек в муниципальных органах власти и организациях выросло, что связано с низким уровнем осведомленности о киберугрозах, низкими инвестициями в безопасность и использованием устаревших средств защиты[278].

Официально в 2024 году Роскомнадзор зафиксировал 135 утечек, содержащих свыше 710 миллионов записей о россиянах. В 2025 году количество зафиксированных случаев компрометации баз персональных данных в России снизилось до 118, в сеть попали более 52 миллионов записей. По данным аналитиков компании «Еса Про» (входит в ГК «Кросс технолоджис»), лидером по числу утечек в 2025 году стал госсектор – на него пришлось 73% всех случаев. Наибольший объём утечек был зафиксирован в данной категории: он превысил 105 млн строк данных о пользователях и компаниях. Значительная доля также пришлась на ритейл — 19%, тогда как сфера услуг, включая образование, здравоохранение и онлайн-сервисы, заняла третью позицию с показателем 6,5%. В целом за год объём утекших данных превысил 145 млн. строк[279]. Началось применение крупных и оборотных штрафов.[280]

Таким образом, анализ правоприменительной практики и официальной статистики позволяет сделать вывод о результативности публично-правовых мер, принимаемых в России в целях обеспечения безопасности персональных данных. Снижение количества утечек указывает не только на практический эффект таких мер, но и на наличие более системного подхода государства к регулированию данной сферы.

Изучение правоприменительных материалов позволяет сделать вывод о

---

[278] В России за полгода утекло около 1 млрд строк персональных данных. URL: https://www.forbes.ru/tekhnologii/520596-v-rossii-za-polgoda-uteklo-okolo-1-mlrd-strok-personal-nyh-dannyh (дата обращения: 30.12.2024).

[279] Количество утечек персональных данных в 2025 году снизилось до 118. URL: https://www1.ru/news/2026/01/22/v-rossii-v-2025-godu-kolicestvo-utecek-personalnyx-dannyx-snizilos-do-118.html (дата обращения: 30.04.2026).

[280] См.: Решение Арбитражного суда г.Москвы от 5 марта 2026 г. по делу № А40-351064/2025. URL: https://www.garant.ru/files/9/2/2026629/reshenie_arbitragnogo_suda_g_moskvi_ot_5_marta_2026_g_po_delu_n_a40_351064_2025.pdf (дата обращения: 30.04.2026); Решение Арбитражного суда г.Санкт-Петербурга и Ленинградской области от 10 марта 2026 г. по делу № А56-4733/2026. URL: https://www.garant.ru/files/9/2/2026629/reshenie_arbitragnogo_suda_g_sankt_peterburga_i_leningradskoy_oblasti_ot_10_marta_(1).pdf

неоднородности судебной практики Российской Федерации по делам, связанным с нарушением законодательства о персональных данных.[281] На этом фоне возрастает роль Роскомнадзора как уполномоченного органа, обеспечивающего регулирование отношений в области обработки и защиты персональных данных, а также осуществляющего контроль и надзор за соблюдением соответствующих правовых требований. На современном этапе его полномочия существенно расширены, что позволяет говорить о повышении институциональной значимости данного органа в системе защиты персональных данных. При этом, представляется, что подход Роскомнадзора и судов должен быть сбалансированным для целей формирования последовательной и однородной судебной практики. На примере эффективного противодействия нарушениям в сфере законодательства персональных данных можно говорить и об эффективности работы Роскомнадзора, а также российского судебного правоприменения[282].

**3) Защита персональных данных при раскрытии данных государством в России.** Анализ достаточно большого количества утечек персональных данных из государственного сектора свидетельствует, что в современной России органы государственной и муниципальной власти как операторы персональных данных продемонстрировали недостаточную способность организовать надлежащую защиту персональных данных граждан.[283]

Постановление Правительства РФ «Об обеспечении доступа к общедоступной ин- формации о деятельности государственных органов и органов местного самоуправления в информационно- но-телекоммуникационной сети «Интернет» в форме открытых данных» [284] определяет понятие «открытые

---

[281] Судебная практика по защите персональных данных. URL: https://searchinform.ru/resheniya/biznes-zadachi/zaschita-personalnykh-dannykh/realizaciya-zashchity-personalnyh-dannyh/sudebnaya-praktika-po-zashchite-person alnyh-dannyh/?ysclid=m4p7apk0aj337596097 (дата обращения: 30.12.2024)

[282] Порядок направления запроса, требования к его содержанию, а также требования к форме и содержанию представляемых оператором персональных данных сведений регламентированы частями 3–6 статьи 14 ФЗ о ПДн.

[283] См.: *Поликанина О. А., Поликанин А. Н., Шабурова А. В.* Организация защиты персональных данных в государственных и муниципальных информационных системах // Интерэкспо Гео-Сибирь. 2022. Т. 6. С. 203.

[284] Постановление Правительства РФ от 10.07.2013 г. № 583 «Об обеспечении доступа к общедоступной информации о деятельности государственных органов и органов местного самоуправления в информационно-телекоммуникационной сети «Интернет» в форме открытых данных» // Собрание законодательства РФ. 2013. № 30. Ст. 4107.

данные» и общие правила взаимодействия с ними на российском национальном уровне, включая необходимость публикации. Отдельные нормативные правовые акты устанавливают различные виды доступа к данным, которые определяют, в том числе возможность их публикации в открытом доступе. При этом устанавливаются различные категории доступности (доступа): полностью свободный, частично свободный и полностью закрытый. В связи с этим приняты акты для обеспечения доступа открытых данных, включая ряд федеральных законов[285] и другие нормативные акты[286], разработанные Правительством РФ и федеральными органами исполнительной власти.

Кроме того, также приняты различные нормативные правовые акты, определяющие ограничение доступа к отдельным видам информации ограниченного доступа, в том числе тайнам[287]. В рамках современных справочных правовых систем России производится систематизация таких видов информации ограниченного доступа[288]. Формирование политик по обеспечению открытости данных осуществляется и в рамках различных планов, устанавливаемых органами власти[289].

Согласно данным компании SearchInform, наблюдается постоянный рост числа инцидентов, связанных с утечкой персональных данных.[290] При этом значительная доля таких утечек происходит в государственных учреждениях,

---

[285] Включается Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3448.; Федеральный закон от 9 февраля 2009 г. №8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» // Собрание законодательства РФ. 2009. № 7 (1 ч.). Ст. 776 др.

[286] Например, Постановление Правительства Российской Федерации от 24 ноября 2009 г. №953 «Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти»; Распоряжение Правительства Российской Федерации от 10 июля 2013 г. №1187-р «О перечнях информации о деятельности государственных органов, органов местного самоуправления, размещаемой в сети «Интернет» в форме открытых данных» // СПС «КонсультантПлюс» и др.

[287] См., например: Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» // Собрание законодательства РФ. 2011 . №48. Ст. 6724.

[288] См., например: Перечень нормативных актов, относящих сведения к категории ограниченного доступа (Матери ал подготовлен специалистами КонсультантПлюс). URL: https://www.consultant.ru/document/cons_doc_LAW_93980/ (дата обращения: 03.01.2025).

[289] Например, планы открытости; планы информатизации; планы развития официальных сайтов; планы мероприяти й отдельных программ и ведомств. URL: https://www.infoculture.ru/wp-content/uploads/2020/11/OpenDataReview.pdf?ysclid=m5g7h5i5rb806775419 (дата обращения: 03.01.2025).

[290] Увеличение количества инцидентов, связанных с утечкой персональных данных, с 2017 по 2019 г.г. составило порядка 20-23 % ежегодно. В 2020 г. данный показатель вырос до 33 %. Источник данных: Исследование уровня информационной безопасности российских компаний с 2017 по 2019 г.г. URL: https://searchinform.ru/research (дата обращения: 03.01.2025).

осуществляющих обработку персональных данных.[291]

Особенности обработки персональных данных в государственных системах персональных данных прямо закреплены в статье 13 Закона РФ о персональных данных. Следует отметить, что в России в последние годы был приняты ряд нормативных правовых актов, направленных на обеспечение безопасности персональных данных при их использовании государством.[292]

На сегодняшний день проблема утечки персональных данных из государственных и муниципальных информационных систем является актуальной и, по мнению некоторых российских ученых, связана с тем, что в информационных системах органов власти общедоступные сведения и сведения ограниченного доступа не разграничены между собой техническими и организационными средствами защиты[293].

Следует отметить, что в последние годы на территории Российской Федерации произошли значительные изменения в публично-правовом обеспечении безопасности персональных данных граждан при оказании государственных и муниципальных услуг. На государственные органы, выступающие в качестве операторов персональных данных, возложены дополнительные обязанности по защите и обработке таких данных. Для повышения эффективности деятельности федеральных органов исполнительной власти и органов местного самоуправления представляется необходимым осуществлять постоянный мониторинг изменений законодательства в данной сфере [294] и его развитие.

---

[291] См.: Глобальное исследование уровня информационной безопасности в компаниях России и СНГ за 2020 – 2022 годы. URL: https://searchinform.ru/survey/global (дата обращения: 03.01.2025).

[292] См.: Федеральный закон «О внесении изменений в Федеральный закон "О персональных данных", отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона «О банках и банковской деятельности» от 14.07.2022 № 266-ФЗ (последняя редакция) // Собрание законодательства РФ. 2022. № 29 (ч. III). Ст. 5233; и др.

[293] *Поликанина О. А., Поликанин А. Н., Шабурова А. В.* Организация защиты персональных данных в государственных и муниципальных информационных системах // Интерэкспо. Гео-Сибирь. 2022. Т. 6. С. 197.

[294] Новации в сфере обработки и защиты персональных данных. URL: https://bftcom.com/expert-bft/28248/ (дата обращения: 31.12.2024).

## 2.3 Информационно-правовое обеспечение безопасности персональных данных в России

В Российской Федерации формирование и развитие института правового регулирования персональных данных осуществляется преимущественно в рамках информационного права. Данный подход предполагает рассмотрение персональных данных как особого вида информации, требующего установления специального правового режима, в первую очередь публично-правового, непосредственно направленного на обеспечение безопасности персональных данных. Установление такого специального публично-правового режима персональных данных уже выступает одной из ключевых публично-правовых мер обеспечения безопасности персональных данных, которая позволяет в рамках публичного законодательства формировать систему специальных правовых норм, а также специальных правовых средств (правовые принципы, специальные контрольно-надзорные меры, меры обеспечения конфиденциальности и др.), направленных на обеспечение безопасности персональных данных.

Важным этапом в становлении данной системы информационно-правового обеспечения безопасности персональных данных стало принятие Постановления Правительства РФ от 15.04.2014 № 313 «Об утверждении государственной программы Российской Федерации «Информационное общество»»[295], которое закрепило стратегические направления развития цифровой инфраструктуры и создания условий для безопасного обращения персональных данных. Реализация данной программы предусматривала обновление нормативно-правовой базы, развитие механизмов защиты информации и создание условий для повышения доверия к цифровым технологиям. Важное место в ней занимали меры, связанные с безопасным использованием информационно-телекоммуникационных технологий, что оказало прямое влияние на формирование современных подходов к защите персональных данных. Тем самым программа способствовала выработке

[295] Постановление Правительства РФ от 15.04.2014 № 313 «Об утверждении государственной программы Российской Федерации «Информационное общество» (с изм. и доп., вступ. в силу с 01.01.2023) // Собрание законодательства РФ. 2014. № 18 (2 ч.). Ст. 2159.

более целостной модели регулирования цифровой среды, в рамках которой защита персональных данных стала рассматриваться как необходимый элемент развития информационного общества в России.

До принятия Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» регулирование обращения с персональной информацией в Российской Федерации было рассредоточено по различным нормативным правовым актам и не образовывало единой системы. Принятие указанного закона стало важным этапом в развитии правового механизма защиты персональных данных, поскольку закрепило их как самостоятельный объект правовой охраны в условиях расширения цифровых технологий. При этом законодательство о персональных данных следует рассматривать как часть информационного законодательства, имеющего комплексный характер и объединяющего нормы различных отраслей российского права[296]. Существенное значение для развития системы защиты персональных данных имело Постановление Правительства РФ от 21.03.2012 № 211[297], которым был установлен перечень мер, направленных на обеспечение соблюдения требований законодательства государственными и муниципальными органами. Указанный акт конкретизировал организационные и технические обязанности, связанные с обработкой персональных данных: принятие соответствующей политики, назначение ответственных лиц, регулирование доступа к информации и контроль за выполнением внутренних процедур. Особенность постановления состоит в его специальной сфере действия, поскольку оно адресовано исключительно государственным и муниципальным органам. Это позволяет рассматривать его как один из инструментов формирования особого режима защиты персональных данных в публичном секторе. В более широком смысле постановление отражает постепенное усложнение правового регулирования с учётом технологического развития и

[296] *Терещенко Л. К.* Модернизация информационных отношений и информационного законодательства: монография. М.: Институт законодательства и сравнительного правоведения при Правительстве РФ: ИНФРА-М, 2013. Доступ из СПС «КонсультантПлюс». URL: http://www.izak.ru/upload/iblock/d9a/d9a41cd976d8a127e078656536b0cc30.pdf.

[297] Постановление Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» // Собрание законодательства РФ. 2012. № 14. Ст. 1626.

практики применения законодательства.

В системе информационного права ФЗ о ПДн выполняет системообразующую функцию, выступая не просто одним из нормативных правовых актов, а центральным элементом, вокруг которого формируется комплексный институт правового регулирования персональных данных.

Одной из ключевых мер по обеспечению безопасности персональных данных, реализованных в рамках ФЗ о ПДн, стало формирование универсального понятийного аппарата. В частности, статья 3 данного закона закрепила официальные определения, которые стали основополагающими для последующего развития правовых конструкций в данной области. ФЗ о ПДн устанавливает максимально широкое определение персональных данных как «любой информации, относящейся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных)».[298] Данная формулировка, соответствующая международным подходам к определению персональных данных, обусловливает обширную сферу применения законодательства о персональных данных.

Помимо прочего, ФЗ о ПДн ввел ключевые термины, такие как «оператор», «обработка персональных данных» (включающая весь жизненный цикл персональной информации), «трансграничная передача персональных данных» и «обезличивание персональных данных». Унификация используемой терминологии способствовала устранению правовой неопределённости и заложила основу для единообразного толкования и применения нормативных положений.

Следующей важной публично-правовой мерой обеспечения безопасности персональных данных, установленной в рамках информационного права, необходимо выделить систему фундаментальных принципов обработки персональных данных (статья 5 ФЗ о ПДн), которые служат правовым ориентиром для всех операторов. Причем анализ китайского законодательства в сфере персональных данных также позволяет говорить, что это базовая публично-

[298] П. 1 ст. 3 Федерального закона «О персональных данных».

правовая мера обеспечения безопасности персональных данных.

К числу указанных принципов относятся законность и добросовестность обработки, ограничение целей обработки конкретными и заранее определёнными задачами, соразмерность объёма и характера обрабатываемых данных поставленным целям, а также обеспечение точности и актуальности персональных данных. Кроме того, статьи 6, 9–11 ФЗ о ПДн детально регламентируют условия законности обработки персональных данных, устанавливая исчерпывающий перечень оснований, среди которых ключевое значение имеет добровольное согласие субъекта.

Принципы обработки персональных данных носят универсальный характер, поскольку распространяются на весь спектр отношений, складывающихся в процессе обработки персональных данных, как только они обособляются от субъекта. Они не распространяются на отношения, которые не являются предметом регулирования ФЗ о ПДн и прямо предусмотрены им. Анализ законодательства о персональных данных и соответствующей правоприменительной практики также свидетельствует, что принципы обработки персональных данных применяются независимо от:

- субъекта персональных данных, субъекта, осуществляющего обработку персональных данных;

- способа обработки персональных данных (ч. 3 ст. 4 ФЗ о ПДн устанавливает, что особенности обработки персональных данных, осуществляемой без использования средств автоматизации, могут быть установлены федеральными законами и иными нормативными правовыми актами Российской Федерации с учетом положений ФЗ о ПДн);

- конкретных действий (операций) или совокупности действий (операций) с персональными данными (сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение и др.;

- территории обработки (распространение на трансграничную обработку).

Принципы обработки персональных данных – это совокупность идей, начал, универсально распространяемых на все отношения, складывающиеся в сфере обработки персональных данных, а также оказывающих непосредственное влияние на законодательство о персональных данных и правоприменительную практику в сфере обеспечения безопасности персональных данных.

Их значение проявляется в том, что они:

- являются базовыми началами, на основе которых формируется и развивается система правового регулирования персональных данных;

- являются обязательными требованиями, которые должны соблюдаться всеми участниками отношений в сфере персональных данных в Российской Федерации, а также система защиты персональных данных[299];

- нарушение принципов обработки персональных данных является основанием для привлечение к юридической ответственности;

- неразрывно связаны с другими правилами. Основным условием обработки персональных данных является то, что она должна осуществляться с соблюдением принципов и правил, предусмотренных Федеральным законом «О персональных данных» (ч. 1 ст. 6);

- дисциплинируют участников отношений в сфере персональных данных, формируется культура обработки персональных данных. Являются связующим началом, объединяющим правовые и этические нормы регулирования персональных данных[300].

Одним из ключевых вопросов, возникающих при построении современной системы принципов обработки персональных данных является вопрос о исчерпывающем характере принципов, содержащихся в статье 5 ФЗ о ПДн. В частности в России прямо не предусмотрено в ст. 5, но закрепляется в ст. 7 ФЗ о ПДн («Конфиденциальность персональных данных») положение, что «операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта

[299] *Ван Гуанлун.* Административно-правовые меры по обеспечению безопасности персональных данных при раскрытии информации правительством в Китае. // Вестник Санкт-Петербургского университета. Право. 2024. № 3. С. 815-834.

[300] См.: Право персональных данных: учебник / под общ. ред. *А.В. Минбалеева*. Саратов: Амирит, 2023. С. 34-35.

персональных данных, если иное не предусмотрено федеральным законом». Полагаем, что данное положение представляет собой отдельный принцип обработки персональных данных – принцип обеспечения конфиденциальности персональных данных. Статья 7 ФЗ О ПДн находится в разделе «Принципы и условия обработки персональных данных». Данное начало как раз обеспечивает главную особенность персональных данных как вида информации ограниченного доступа, - распространение на них режима конфиденциальности и необходимости его соблюдения, независимо от того, были ли они раскрыты субъектом персональных данных или нет. Данный принцип предполагает и недопустимость разглашения конфиденциальности, и влияет на развитие законодательства о персональных данных сквозь призму обеспечения их конфиденциальности и оказывает воздействие на правоприменителя при разрешении конкретных споров.

Также законом предусмотрен особый режим обработки биометрических данных и специальных категорий персональных данных (статьи 10, 11), что подчеркивает необходимость принятия при обеспечении их безопасности дополнительных мер. Формирование специальных правовых режимов для отдельных категорий персональных данных выступает особым правовым средством, направленным на обеспечение безопасности наиболее уязвимых и чувствительных данных.

Особое значение как информационно-правовая мера обеспечения безопасности персональных данных имеет закрепление в статьях 14–17 Федерального закона о персональных данных системы прав субъекта персональных данных. К ним относятся право на доступ к персональным данным, их уточнение, блокирование и уничтожение, а также право на отзыв согласия на обработку. Тем самым конституционное право на неприкосновенность частной жизни, предусмотренное статьёй 23 Конституции Российской Федерации, получает развитие в виде конкретных правомочий и гарантий в сфере обработки персональных данных.

Системообразующее значение Федерального закона о персональных данных выражается, в частности, в создании правового механизма контроля за

соблюдением требований в данной сфере. Важным элементом этого механизма стало закрепление за Роскомнадзором полномочий уполномоченного органа по защите прав субъектов персональных данных, что предусмотрено статьёй 23 указанного закона. Последующее развитие данного направления связано с приказом Роскомнадзора от 27.10.2022 № 178[301], утвердившим методику оценки потенциального вреда субъектам персональных данных при нарушении законодательства. Данный нормативный акт детализирует критерии оценки тяжести последствий нарушений законодательства о персональных данных, классифицируя возможный вред по степени его влияния на права и законные интересы граждан. Одновременно он определяет порядок расчёта рисков причинения такого вреда. Закреплённые требования имеют значение для практики контрольной деятельности Роскомнадзора, поскольку позволяют учитывать характер и масштаб возможных последствий при оценке выявленных нарушений. Наряду с этим статья 23.1 Федерального закона о персональных данных наделяет Роскомнадзор полномочиями по проведению проверок, выдаче предписаний и привлечению к ответственности. Эти положения в совокупности обеспечивают развитие публично-правового механизма контроля за соблюдением законодательства о персональных данных и создают дополнительные гарантии защиты прав их субъектов.

Принятие Федерального закона о персональных данных стало важным фактором дальнейшей систематизации российского законодательства в рассматриваемой сфере. На его основе получили развитие специальные составы административных правонарушений, закреплённые в главе 13 Кодекса Российской Федерации об административных правонарушениях, посвящённой нарушениям в области связи и информации. Кроме того, положения данного закона были последовательно интегрированы в отраслевое законодательство, включая главу 14 Трудового кодекса Российской Федерации, федеральные законы «О связи», «О банках и банковской деятельности» и иные нормативные правовые

[301] Приказ Роскомнадзора от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»» // Справочная правовая система «Консультант Плюс».

акты.

Современное правовое регулирование персональных данных в Российской Федерации представляет собой многоуровневую систему, сформировавшуюся под влиянием международных стандартов и национальной правовой традиции. Как было отмечено ранее, её основу составляет Федеральный закон о персональных данных, закрепляющий ключевые принципы и механизмы публично-правового обеспечения безопасности персональных данных. Регулирование персональных данных в российском праве следует рассматривать как комплексный институт информационного права [302], объединяющий нормы общего и специального характера. Его содержание охватывает не только базовые требования к обработке и защите персональных данных, но и особенности правового режима отдельных категорий информации, а также специфику их использования в различных сферах общественных отношений.

Характерной чертой указанной системы является её многоуровневая структура, при которой конституционные положения о праве на неприкосновенность частной жизни выступают в качестве базовой правовой основы и конкретизируются в отраслевом законодательстве. В последние годы возрастает значение подзаконного регулирования и ведомственных рекомендаций, что позволяет быстрее реагировать на изменения, обусловленные развитием цифровых технологий. При этом целостность правовой системы сохраняется за счёт соподчинённости нормативных актов и их содержательной взаимосвязи.

Существенное значение в системе защиты персональных данных имеет деятельность Роскомнадзора как уполномоченного органа, отвечающего за обеспечение прав субъектов персональных данных.[303] Его роль не ограничивается контролем и надзором за соблюдением законодательства: особое место занимает работа по формированию отраслевых стандартов обработки персональной информации. Такие стандарты способствуют унификации требований к обработке данных в различных секторах экономики и позволяют адаптировать общие

[302] Право персональных данных : учебник / под ред. д-ра юрид. наук, профессора *А. В. Минбалеева*. 2-е изд., доп. и перераб. М. : Издательский центр Университета имени О.Е. Кутафина (МГЮА), 2025. С. 9.

[303] Роскомнадзор создаёт отраслевые стандарты для работы с персональными данными. URL: https://mastertel.ru/ru/news/159 (дата обращения: 31.10.2025).

положения законодательства к особенностям конкретных сфер деятельности. Отраслевые стандарты Роскомнадзора позволяют адаптировать общие положения законодательства к особенностям конкретных отраслей и одновременно закрепляют единые методические ориентиры в области защиты персональных данных. В результате они способствуют более упорядоченной организации сбора и обработки персональной информации, повышению ответственности операторов и укреплению прозрачности правового регулирования в данной сфере [304]. Это способствует повышению уровня защищённости персональных данных и одновременно формирует более единое правовое пространство цифровой экономики, основанное на балансе между технологическим развитием и защитой прав граждан. Не случайно в монографии «Правовое регулирование оборота персональных данных в условиях современных вызовов и угроз» позиция Роскомнадзора анализируется более чем в тридцати контекстах, что свидетельствует о его заметной роли в развитии современного регулирования персональных данных [305]. Институциональная структура регулирования персональных данных не ограничивается осуществлением государственного контроля и надзора. Она также включает методическое сопровождение операторов, консультирование участников соответствующих правоотношений и обеспечение защиты прав субъектов персональных данных. В последние годы особое значение приобретает межведомственное взаимодействие, связанное с обеспечением национальной безопасности и противодействием новым угрозам в цифровой среде. Такой подход был закреплён, в частности, в Указе Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» [306]. В данном стратегическом документе цифровая трансформация отнесена к числу существенных вызовов современного развития, что обусловливает необходимость согласованных действий со стороны

[304] Отраслевые стандарты Роскомнадзора помогут упорядочить сбор персональных данных и усилят ответственность операторов. URL: https://kritbi.ru/cssi-news/otraslevye-standarty-roskomnadzora-pomogut-uporjadochit-sbor-personalnyh-dannyh-i-usiljat-otvetstvennost-operatorov/ (дата обращения: 31.10.2025).

[305] Правовое регулирование оборота персональных данных в условиях современных вызовов и угроз: монография / под общ. ред. А.В. Минбалеева. Саратов : Амирит, 2023.

[306] Указ Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // Доступ из справ.-правовой системы «КонсультантПлюс».

различных государственных институтов. Важное место занимает развитие национальной инфраструктуры защиты персональных данных, а также укрепление механизмов противодействия киберугрозам. Соответственно, особую актуальность приобретает координация деятельности правоохранительных органов, регулирующих структур и субъектов критической информационной инфраструктуры.

Российское законодательство о персональных данных в последние годы развивается под прямым влиянием цифровых технологий. Обработка данных уже не ограничивается традиционными информационными системами, а всё чаще связана с большими данными, интернетом вещей и искусственным интеллектом. Поэтому правовое регулирование постепенно дополняется специальными режимами, рассчитанными на новые технологические практики. Вместе с тем такие изменения не отменяют базового требования: развитие цифровой экономики должно соотноситься с защитой прав граждан, конфиденциальностью и безопасностью персональных данных.

Практика применения законодательства о персональных данных в судах позволяет увидеть, как общие нормы работают в конкретных ситуациях. В судебных решениях постепенно формируются подходы к вопросам разграничения персональных и обезличенных данных, а также к определению границ допустимой обработки информации. Эти подходы имеют значение не только для правоприменения, но и для дальнейшего развития законодательства, поскольку показывают, какие положения требуют уточнения.

Перспективы развития регулирования персональных данных во многом зависят от того, насколько последовательно будут решаться проблемы, возникающие в условиях цифровизации. Среди них особое значение имеет согласование классических принципов защиты персональных данных с практическими потребностями цифровой экономики. Не менее важной остаётся выработка правовых подходов к новым технологиям, которые меняют способы сбора, анализа и использования информации. При этом ориентация на международные стандарты должна сочетаться с учётом национальных правовых

особенностей и интересов Российской Федерации.

Комплексные требования к обеспечению безопасности персональных данных при их обработке

В настоящее время объективной реальностью является необходимость обеспечения безопасности персональных данных, поскольку информация о человеке превратилась в дорогой товар[307]. Современная система обеспечения безопасности персональных данных в Российской Федерации представляет собой многоуровневый механизм правового регулирования, охватывающий различные аспекты обработки и защиты информации. Основные требования закреплены в ФЗ о ПДн, который устанавливает обязанность операторов принимать необходимые организационные и технические меры для предотвращения несанкционированного доступа к персональным данным и их неправомерной обработки. Система защиты персональных данных включает совокупность правовых, организационных и технических мер, разрабатываемых с учётом актуальных угроз информационной безопасности и особенностей используемых информационных технологий[308].

В области организационно-правовых мер обеспечения безопасности первостепенное значение имеют меры по разработке внутренней документации, определяющей политику обработки персональных данных. К таким мерам относится назначение ответственных должностных лиц, утверждение регламентов доступа к информации, а также формирование системы внутреннего контроля. Особое внимание уделяется процедурам регулярного аудита и оценки соответствия процессов обработки установленным нормативным требованиям, включая соблюдение Постановления Правительства РФ от 16.01.2023 № 24 «Об утверждении Правил принятия решения уполномоченным органом по защите прав субъектов персональных данных о запрещении или об ограничении трансграничной передачи персональных данных в целях защиты нравственности,

[307] Федеральный закон «О персональных данных»: научно-практический комментарий (постатейный) / *А. Х. Гафурова, Е. В. Доротенко, Ю. Е. Контемиров* [и др.]; под ред. *А. А. Приезжевой.* М.: Редакция «Российской газеты», 2015. Вып. 11. Доступ из СПС «КонсультантПлюс». URL: https:// www.tgl.net.ru/files/bezopasno/fz-pd-11.pdf.

[308] Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к за щите персональных данных при их обработке в информационных системах персональных данных» // СЗ РФ. 2012. № 45. Ст. 6257.

здоровья, прав и законных интересов граждан»[309]. Указанный нормативный акт определяет критерии допустимости трансграничной передачи данных и тем самым возлагает на операторов обязанность учитывать соответствующие риски в системе внутреннего контроля. Прежде всего имеются в виду риски, способные затронуть охрану основных конституционных ценностей. В связи с этим передача данных за пределы национальной юрисдикции должна сопровождаться предварительной оценкой возможных последствий. Такая оценка позволяет соотнести права субъектов персональных данных с публичными интересами государства в сфере цифровой безопасности.

Технические меры защиты персональных данных включают использование специальных средств информационной безопасности, в том числе шифрования, обезличивания, резервного копирования и восстановления информации. Особую значимость они приобретают при трансграничной передаче данных и размещении информации в облачных средах, где риски не ограничиваются внутренней инфраструктурой оператора. Поэтому такие меры должны применяться системно, сопровождаться регулярным контролем и пересматриваться по мере появления новых угроз безопасности персональных данных.

В системе защиты персональных данных существенное значение имеет предварительная оценка рисков и возможного ущерба, который может возникнуть при нарушении безопасности информации. Законодательство ориентирует операторов на анализ актуальных моделей угроз при определении необходимых мер защиты. В результате требования к безопасности применяются не единообразно, а с учётом условий обработки, характера персональных данных и уровня риска, связанного с их использованием.

Интенсивное развитие цифровых технологий требует постоянного совершенствования механизмов защиты персональных данных. На первый план выходят разработка специальных стандартов информационной безопасности для новых технологий обработки данных и внедрение риск-ориентированных

[309] Постановление Правительства РФ от 16.01.2023 № 24 «Об утверждении Правил принятия решения уполномоченным органом по защите прав субъектов персональных данных о запрещении или об ограничении трансграничной передачи персональных данных в целях защиты нравственности, здоровья, прав и законных интересов граждан» // Собрание законодательства РФ. 2023. № 4. Ст. 644.

подходов к регулированию. Эти меры призваны обеспечить разумное соотношение между защитой прав и свобод граждан и условиями дальнейшего технологического развития.

Таким образом, исследования в области защиты персональных данных в Российской Федерации развиваются в рамках информационного права. Данный подход предполагает рассмотрение персональных данных как особого вида информации ограниченного доступа, требующей установления специального правового режима. Именно в рамках информационного права в России выстраивается основной набор публично-правовых мер обеспечения безопасности персональных данных: базовые правовые нормы, публично-правовой режим персональных данных, специальные правовые режимы отдельных видов персональных данных, понятийный аппарат, принципы обработки персональных данных, система прав и обязанностей участников отношений в сфере персональных данных, система специальных мер обеспечения безопасности персональных данных и др.

Исследование принципов обработки персональных данных в России и Китае позволило обосновать, что принципы обработки персональных данных выступают одной из базовых публично-правовых мер обеспечения безопасности персональных данных как в Российской Федерации, так и в Китайской Народной Республике. Они представляют собой совокупность идей, начал, универсально распространяемых на все отношения, складывающиеся в сфере обработки персональных данных, а также оказывающих непосредственное влияние на законодательство о персональных данных и правоприменительную практику в сфере обеспечения безопасности персональных данных. Установлено, что в качестве самостоятельного принципа обработки персональных данных в России необходимо рассматривать принцип обеспечения конфиденциальности персональных данных (в Китае он обозначен как принцип обеспечения безопасности).

Данный принцип обеспечивает реализацию главной особенности персональных данных как вида информации ограниченного доступа –

распространение на них режима конфиденциальности и необходимости его соблюдения, независимо от того, были ли они раскрыты субъектом персональных данных или нет. Он предполагает недопустимость утраты конфиденциальности персональных данных, влияет на развитие законодательства о персональных данных в части обеспечения их конфиденциальности, а также оказывает воздействие на правоприменение при разрешении конкретных споров в сфере персональных данных.

В отличие от российской модели, китайская научная парадигма изначально сформировалась в контексте конституционного и административного права. Это обуславливает доминирование публично-правового подхода к регулированию персональных данных, при котором основной акцент делается на защите государственных интересов и обеспечении национальной безопасности. Конституционное закрепление права на неприкосновенность частной жизни в статье 40 Конституции КНР конкретизируется в отраслевом законодательстве, где приоритет отдается вопросам административного контроля и соблюдения публичных интересов.

В настоящее время в Китае наблюдается формирование новой научной тенденции – активное развитие цифрового права как самостоятельного направления юридических исследований. В рамках данной парадигмы персональные данные рассматриваются комплексно, во взаимосвязи с такими феноменами цифровой трансформации, как большие данные, искусственный интеллект и алгоритмическое управление. Данный подход способствует синтезу методов различных отраслей права с целью выстраивания сбалансированной системы регулирования, адекватно отвечающей вызовам цифровой трансформации государства, общества и права.

# ГЛАВА III. ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ПУБЛИЧНО-ПРАВОВОГО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В КИТАЕ И РОССИИ

## 3.1 Формирование и развитие права на персональные данные в Китае и России как меры обеспечения безопасности персональных данных

Представленный выше анализ демонстрирует следующие различия в защите персональных данных, закрепленные в конституциях Китая и России.

1) Различия конституционных норм в указанной сфере.

Как известно, в понятии достоинства личности сфокусировано множество базовых правовых характеристик, таких как возможность быть предпосылкой и основой прав человека, критерием эффективности права и государства, общеправовым принципом, стержневой основой правотворчества, правоприменительной и правоохранительной деятельности и т. д., что позволяет говорить о его исключительной правовой ценности[310].

В Китае аргумент о том, что право на личную информацию защищено Конституцией, основан на положении о правах человека, содержащемся в статье 33, и на положении о человеческом достоинстве, содержащемся в статье 38. Иными словами, основываясь на разумных доводах и достаточном толковании двух вышеуказанных статей, можно сделать вывод, что право на персональную информацию относится к категории основных прав. Соответственно, право на свободу личности (ст. 37), право на неприкосновенность жилища (ст. 39) и право на свободу корреспонденции (ст. 40) служат для закрепления статуса вышеупомянутого конституционного права.

Гуманистическая идея ценности человеческой личности и её достоинства находит своё отражение в статье 2[311] и части 1 статьи 21[312] Конституции Российской Федерации. Что касается конституционных мер защиты персональных

---

[310] *Оботурова Н.С.* Концепт достоинства человека и его нравственно-правовое значение // Сетевой научно-практический журнал частного и публичного права. 2022. № 5 (20). С. 28.

[311] Статья 2 Конституции РФ гласит: «Человек, его права и свободы являются высшей ценностью. Признание, соблюдение и защита прав и свобод человека и гражданина – обязанность государства».

[312] Часть 1 статьи 21 Конституции РФ регламентирует: «Достоинство личности охраняется государством. Ничто не может быть основанием для его умаления».

данных в России, то они основаны на нормах, предусмотренных частями 1 и 2 статьи 23, части 1 статьи 24 и статье 25 Конституции РФ.[313] Российская конституционно-правовая модель защиты персональных данных основана на понимании персональных данных как объекта правовой защиты. В частности, ключевым элементом данной модели является право на неприкосновенность частной жизни, закреплённое в части 1 статьи 23 и части 1 статьи 24 Конституции Российской Федерации.

Особенности российской модели конституционной защиты персональных данных проявляются через гарантии права на неприкосновенность частной жизни. В Китае конституционная модель защиты персональных данных основывается на принципе неприкосновенности человеческого достоинства, который прямо закреплен в Конституции. Сравнительный анализ показывает, что конституционная защита права на персональные данные в Китае имеет более абстрактный характер по сравнению с российской моделью.

2) Различия в механизме конституционного контроля. Вышеизложенное показывает, что в России именно с помощью метода конституционного контроля решается вопрос о том, имеет ли место нарушение Конституции РФ при рассмотрении дел, связанных с персональными данными граждан. Согласно духу и принципам Конституции Китая, законы, постановления, подзаконные акты и любые нормативные документы не должны противоречить Конституции, но в настоящее время не имеется механизма для подходящего решения проблем, связанных с нарушением Конституции КНР. Поэтому проблема нарушений конституции не может быть принципиально решена[314].

Прошло более 40 лет с момента принятия и имплементации Конституции в 1982 г. в Китае не было ни одного дела, связанного с проверкой конституционности. Фактически, с момента принятия первой Конституции КНР в 1954 г. до сих пор не было ни одного дела о проверке конституционности, однако,

---

[313] То есть: нормы о праве на неприкосновенность частной жизни (ч. 1 ст. 23 в совокупности с ч. 1 ст. 24 Конституции РФ), праве на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ч. 2 ст. 23 Конституции РФ) и о праве на неприкосновенность жилища (ст. 25 Конституции РФ).

[314] *Ван Лэй.* Достижения и проблемы, связанные с конституционными гарантиями основных прав граждан // Гуандунские общественные науки. 2013. № 3. С. 225.

это не значит, что в реальной жизни не было фактов или явлений, нарушающих конституцию. Граждане не раз обращались в Постоянный комитет Всекитайского собрания народных представителей с заявками, в которых рекомендуют отменить неконституционные законы или подзаконные акты, но от Постоянного комитета Всекитайского собрания народных представителей до сих пор не было получено никакого официального ответа на эти заявки[315]. Когда имеет место нарушение конституции, субъект, ответственный за нарушение конституции, самостоятельно отменяет соответствующий нормативный акт, чтобы устранить такое нарушение. Ниже приведен пример применения метода самокоррекции для решения этого рода проблемы:

Дело Сунь Чжигана[316] в 2001 году привело к тому, что 18 июня 2003 года Государственный совет КНР отменил «Правила содержания по стражей и вывоза» 1982 года и заменил их другим нормативным актом[317]. История инцидента с Сунь Чжиганом такова：в 10 часов 17 марта 2001 года Сунь Чжиган, 27-летний специалист по искусству и дизайну, окончивший Уханьский институт науки и технологий, был отправлен полицией полицейского участка Хуанцзе Управления общественной безопасности района Тяньхэ в центр содержания и эвакуации из-за того, что он не взял с собой на улицу никаких документов. Он был переведен в приют в Гуанчжоу. Вечером 18 марта Сунь Чжиган сказал, что ему стало плохо, и его отправили на лечение в специальное лечебное место при муниципальном управлении здравоохранения. В период с 1:13 до 30 утра 20 марта Сунь Чжиган был дважды избит несколькими лицами, поступившими на лечение, одной и той же палаты. В 10:20 утра того же дня Сунь Чжиган получил обширное повреждение мягких тканей и скончался от травматического шока.

---

[315] *Ван Гуанлун.* Административно-правовые меры по обеспечению безопасности персональных данных при раскрытии информации правительством в Китае. // Вестник Санкт-Петербургского университета. Право. 2024. № 3. С. 815-834.

[316] См.: Пекинская газета молодежи, 14 мая 2003 года.

[317] В связи с ограничениями личностной свободы граждан, неясностью условий высылки и злоупотреблением властью в процессе реализации положений «Правил содержания по стражей и вывоза» соответствующие ведомства приняли решение отменить эти Правила «Мерами по спасению бездомных попрошаек, живущих в городе» для защиты законных прав и интересов граждан и обеспечения верховенства закона. См.: Причины отмены «Правил содержания по стражей и вывоза». URL: https://ailegal.baidu.com/?fr=seo_qadetail&template=business&articleType=qadetail&articleId=e81ac7746c2ba9000712 (дата обращения: 11.12.2024).

Указанный метод самокоррекции в Китае отличается от системы конституционного контроля, применяемой большинством зарубежных государств (включая Россию). Последняя является методом внешнего контроля, то есть путем выявления нарушений конституции по делу и пересмотра соответствующих нормативных актов. Исходя из этого, полагаем, что сегодня необходимо говорить о возможности перенять в Китае российский опыт в этой части и создать систему конституционного контроля, соответствующую его национальным условиям, с тем чтобы нарушения конституции, включая случаи нарушения конституционных прав на персональные данные, могли разрешаться своевременно, эффективно и справедливо[318].

Представляется, что принимая во внимание вышеизложенную ситуацию, модель конституционного контроля Китая должна быть построена и усовершенствована на основе анализа российского опыта проверки конституционности в области персональных данных и отечественной практики. Тем более, впервые в Отчете 19-го Национального съезда Коммунистической партии Китая был четко предложен рабочий механизм «проверки конституционности», цель которого заключается в усилении контроля за исполнением Конституции и обеспечении ее авторитета[319].

2. Понятие и природа права на персональные данные

Учитывая тот факт, что и в России, и в Китае разработаны специальные законы, которые четко оговаривают защиту прав и интересов, связанных с персональной информацией, возникает необходимость напрямую закрепить право на защиту персональных данных в конституции.[320]

Как упоминалось выше, Китай и Россия в основном основывают концепцию конституционной защиты персональных данных на толковании соответствующих положений своих конституций. В Китае положения Конституции Китайской

---

[318] Как отмечают китайские ученые: «"Дело Сунь Чжигана" привело к созданию механизма конституционного конт роля в Китае и стало органической частью китайской системы конституционного контроля». См.: *Цинь Цяньхун, Д и Гаоян.* Сорок лет системы проверки конституционности в Китае // Академия. 2019. № 4. С. 56.

[319] "Проверка конституционности" — это так важно! Впервые появилась в Отчете о работе 19-го Национального съ езда партии. URL: https://news.cctv.com/2017/12/04/ARTIuU9JgTJPvgSpynMpdAcd171204.shtml (дата обращения: 11. 12.2024).

[320] *Чжан Сян.* Конституционное толкование права на переписку и рамки проверки: обсуждение с Ду Цянцяном, Ва н Каем и Цинь Сяоцзянем // Журнал сравнительного правоведения. 2021. № 1. С. 41-42.

Народной Республики о защите прав человека и человеческого достоинства используются в качестве конституционной основы для защиты персональных данных. Однако положения статьи 33 о правах человека и статьи 38 о человеческом достоинстве являются слишком абстрактными. Иными словами, определение права на персональные данные исключительно через призму права человека и права на человеческое достоинство не обеспечивает достаточного основания для четкой интерпретации, обосновывающей конституционную защиту данного права.

Следовательно, в контексте ценностных принципов прав человека и человеческого достоинства для обоснования конституционной защиты права на персональные данные необходимо опираться на положения, касающиеся более конкретных фундаментальных прав.[321]. Кроме того, права граждан на жилище, свободу и тайну их переписки, предусмотренные статьями 39 и 40 Конституции КНР, относятся к правам и интересам, связанным с неприкосновенностью частной жизни, однако, последняя с персональными данными по содержанию частично совпадает, но не охватывает все аспекты персональных данных[322].

В Российской Федерации право на неприкосновенность частной жизни, право на жилище и право на свободу связи, прямо закрепленные в Конституции РФ, рассматриваются как конституционная основа для защиты персональных данных граждан. Тем не менее, указанные конституционные права не охватывают все аспекты защиты личной информации в полной мере.

Кроме того, права на жилище граждан, свободу и тайну их переписки, предусмотренные в статьях 39 и 40 Конституции КНР, относятся к правам и интересам, связанным с неприкосновенностью частной жизни, однако последнее, имея сквозную взаимосвязь с персональными данными, не охватывает все аспекты персональных данных. По нашему мнению, право на персональные данные должно быть четко закреплено в статье Конституции Китайской Народной

---

[321] *Чжан Сян.* Конституционное подтверждение права на персональную информацию на основе размышления о теории разделения защиты и теории доминирования // Глобальный юридический обзор. 2022. № 1. С. 58-59.

[322] *Ван Гуанлун.* Административно-правовые меры по обеспечению безопасности персональных данных при раскрытии информации правительством в Китае. // Вестник Санкт-Петербургского университета. Право. 2024. № 3. С. 815-834.

Республики, что сможет содействовать:

1) эффективному предотвращению нарушения персональных данных государственными органами и частными обработчиками. В информационную эру правительство постоянно собирает информацию о гражданах в больших масштабах в своей повседневной административной деятельности, и уровень детализации собираемой информации имеет тенденцию к дальнейшему углублению. С развитием технологий его возможности по сбору информации также постоянно возрастают. Тем не менее, регулирование публичной власти, согласно действующему законодательству, остается на уровне защиты гражданских прав против публичной власти, что может затруднять обеспечение его практической эффективности.

Следовательно, возникает необходимость интеграции персональных данных в систему конституционной защиты. Как публичный закон, Конституция регулирует государственную власть для защиты прав и интересов граждан. В случае несоответствия между частными лицами и государственной властью право на персональные данные возводится в ранг Конституции, что может эффективно регулировать обращение с личной информацией со стороны государственной власти, а также побудить государство к активным действиям, гарантирующим реализацию конституционных прав граждан. Именно в этом заключается важное значение конституции по отношению к государственной власти. Кроме того, с учетом значительной «информационной мощи» частных обработчиков информации и неравного статуса между субъектом данных и обработчиком, субъекту персональных данных должна быть предоставлена преимущественная защита, то есть субъекту персональной информации должен быть предоставлен ряд прав, таких как знание, согласие, запрос, копирование и удаление, и реализация этих прав может основываться только на том, что Конституция четко оговаривает права и интересы, связанные с персональными данными [323] . Следовательно, только Конституция может обеспечить самую надежную гарантию

[323] *Ван Сицзинь, Пэн Чжунь.* Конституционная основа правовой системы защиты персональной информации // Цинхуаское право. 2021. № 3. С. 16.

прав и интересов в отношении персональных данных граждан.

2) созданию системы защиты персональных данных, которая будет охватывать всю правовую систему. Помимо того, что основное право в конституции является «субъективным законом» предотвращать незаконное посягательство со стороны государственной власти, оно также является «объективным законом», который может действовать как «объективный ценностный порядок», охватывающий всю правовую систему[324].

В последнем существуют следующие три функции： функция гарантии институциональной системы, то есть государство должно, исходя из значения основных прав, создать соответствующую институциональную систему для реализации требований основных прав и обеспечения реализации ценности основных прав; функция гарантии организационной процедуры, то есть государство должно создать специальные организации и определенные процедуры для реализации духа основных прав; функция предотвращения нарушений, то есть государство должно создать специальную систему и предотвращать нарушение прав личности третьими лицами в ходе функционирования этой системы[325].

Таким образом, если право на персональные данные будет четко закреплено в конституции, оно будет использовано в качестве основы для интеграции существующих положений о защите личной информации, содержащихся в гражданской, уголовной и административной сферах, с тем чтобы права отдельных лиц могли быть согласованы друг с другом для достижения максимальной общей эффективности и создать соответствующие организации и процедуры для реализации положений о защите персональных данных с целью обеспечения систематической защиты личной информации.

3) детализации и конкретизации гарантий прав человека и защиты ценности человеческого достоинства. Человеческое достоинство занимает центральное

---

[324] *Ли Чжунся.* Конституционное закрепление прав на неприкосновенность частной жизни в цифровую эпоху // Журнал Восточно-Китайского политико-юридического университета. 2021. № 3. С. 45.
[325] *Юй Вэньхао.* Основные права. Нанкин: Цзянсуский народное издательство. 2016. С. 47-48.

место в области защиты прав человека [326] . Человеческое достоинство как органическая часть прав человека является открытой и постоянно развивающейся концепцией, а права, связанные с личной информацией, являются воплощением человеческого достоинства в информационную эру. За личной информацией граждан стоит человеческое достоинство. В условиях развития цифровых технологий различные субъекты стремятся собирать персональные данные граждан, и уровень ее детализации достаточен для того, чтобы с помощью данных можно было полностью описать одного конкретного человека. В наши дни нам приходится не только сталкиваться с реальной жизнью, но и принимать во внимание другую «цифровую жизнь» и «цифровую личность», созданные в Интернете. Если такого рода нематериальные данные не регулируются и не защищаются, современная наука и техника могут легко оттолкнуть людей, тем самым лишив их независимости и личностного достоинства как человеческих существ, а также статуса субъекта человека.

Как подчеркивают некоторые ученые, любые нарушения прав человека, совершаемые с использованием информационных технологий, должны рассматриваться как незаконные, и им следует противостоять с помощью щита для защиты прав человека.[327] Включение персональных данных в Конституцию для обеспечения их четкой защиты отражает уважение и защиту человеческого достоинства, отражает внимание Конституции к правам человека, а также закладывает основу для свободного развития человеческой личности в информационную эру.

Все указанные аргументы, на наш взгляд, применимы и к российской системе обеспечения безопасности персональных данных, что также обусловливает возможность рассмотрения в будущем закрепления в Конституции Российской Федерации отдельного права на персональные данные.

В условиях растущего спроса на права в контексте новых технологий вопрос о том, как создать конституционную основу для обеспечения основных прав,

---

[326] *Ли Чжэньшань.* Человеческое достоинство и защита прав человека (переиздание). Тайваньское издательство «Юаньчжао». 2001. С. 03.

[327] *Чжан Вэньсянь.* Нет цифр - нет прав человека. Пекинская ежедневная газета, 2 сентября 2019 года, 15-я страница газеты.

является неизбежной задачей нашего времени. Защита персональных данных на самом деле является требованием к правовому полю, вызванным революционными изменениями в области информационных технологий. В китайской и российской системах конституционных прав рациональное определение местонахождения права на персональные данные тесно связано с тем, как создать интегрированную систему правовой защиты права на личную информацию.

С точки зрения систем основных прав, закрепленных в конституции КНР, следует приложить усилия для того, чтобы право на персональные данные было закреплено в рамках положения о  достоинстве личности как новый тип прав, то есть рассматривать право на персональные данные как одно из прав личности на удовлетворение законных требований о защите личностных интересов в контексте новых технологий и предотвращение вторжения растущих цифровых технологий в пространство для свободного развития личности. Применительно к российской системе в принципе также можно говорить о возможном подходе.

Развитие технологий обработки персональных данных привело к проведению углубленных исследований и анализа отдельных элементов, содержащихся в персональных данных, что в полной мере отражает интересы отдельных лиц, охватываемые личными сведениями. В этом контексте, если Конституция прямо не устанавливает соответствующего права на персональные данные, игнорируя реальные требования к защите права на персональную информацию, обусловленные техническим прогрессом, то защита персональных данных столкнется со многими проблемами.[328] Поэтому существует также необходимость в расширении и обновлении возможных гарантий и ситуаций, которые важно урегулировать в соответствии с положениями Конституции о человеческом достоинстве, поскольку:

1) Индивидуальные свойства персональной информации охватывают личностные интересы отдельного лица, что формирует моральную основу для

[328] *Чжан Сян.* Категория человеческого достоинства в Конституции: на основе защиты личностного права в ГК и персональной информации // Юридические обзоры в Китае. 2023. № 1. С. 63.

защиты права на персональные данные. Публичное свойство личной информации является вторым атрибутом, а индивидуальное свойство - первым. Публичные атрибуты персональной информации являются производными от социальных свойств людей, так что она является не просто символом личности, хобби и данными о поведении, а совокупностью связанных данных, сформированных в ходе социальных взаимодействий. Акцент на публичные свойства личной информации делается для того, чтобы сбалансировать индивидуальные интересы с общественными ценностями, а не для того, чтобы отрицать индивидуальные права. Цифровое развитие не должно быть выше личностной свободы и прав, потому что «ориентация на людей» является фундаментальной ценностной целью развития. Экономическая ценность данных должна основываться на защите личностных прав и интересов субъектов персональных данных, в противном случае она потеряет этическую поддержку[329].

Следовательно, правильное понимание взаимосвязи между двумя атрибутами персональных данных помогает прояснить законодательное основание для их защиты. Сосредоточение внимания на индивидуальных характеристиках персональных данных направлено на защиту человеческого достоинства, содержащегося в персональных данных. Хотя эта защита будет ограничена публичными свойствами персональных данных, ее законность не может быть опровергнута. Как только этическая основа цифрового правосудия будет утрачена, цифровое развитие в конечном итоге уничтожит «человеческое достоинство и свободу» как основные ценности человечества. В условиях развития цифровых технологий необходимо избегать неограниченной обработки персональных данных, что является необходимым условием для свободного развития личности в условиях бесконечно развивающихся технологий обработки данных.[330]

Во-вторых, необходимость прямой защиты прав на персональные данные в рамках конституции заключается в борьбе с ущемлением личностных интересов в результате развития цифровых технологий, чтобы смягчить подавление и

[329] *Чжоу Вэйдун.* Конституционная систематизация прав на персональные данные // Правоведение. 2023. № 1. С. 39.
[330] *Чжао Хун.* От раскрытия информации к защите информации: направление и основные проблемы исследований по защите информационных прав в публичном праве // Журнал сравнительного правоведения. 2017. № 2. С. 31-46.

контроль над индивидуальными правами в результате технического прогресса. Предполагаемая личная информация, полученная в результате чрезмерного сбора и углубленной обработки персональных данных, вызванной использованием больших данных и искусственного интеллекта, серьёзно нарушает автономное пространство отдельных лиц и унижает их личностное достоинство. Нельзя отрицать, что на ранних этапах развития информационных технологий право на персональные данные также может быть включено в существующие рамки защиты неприкосновенности частной жизни, предусмотренные Конституцией. Когда же развитие цифровых технологий выходит за рамки допустимого правом и угрожает человеческому достоинству, необходимо признать рациональность прямой конституционной защиты права на персональные данные, которая направлена на создание механизма по охране прав человека, отвечающего технологическому развитию, с целью того, чтобы сделать все возможное для предотвращения неоправданного ущемления человеческого достоинства применительно к персональным данным.

Следует отметить, что право на персональные данные – это право, которое постепенно раскрывается с развитием цифровых технологий. В настоящее время информационные технологии позволяют за короткий промежуток времени создать цифровую личность, похожую на реальную личность человека. Поскольку данные стали отражением целостной личности человека, защита прав личности должна быть распространена и на персональные данные этого человека [331]. Иными словами, развитие цифровых технологий позволило обработчикам и контролерам персональной информации получить возможность глубокого анализа персональных данных и составления портретов пользователей, которые включают в себя человеческий характер, способности, имущественный статус, сеть социальных связей и многое другое. Развитие цифровых технологий расширило возможности разработчиков и пользователей технологий по сбору, анализу и использованию персональных данных, однако субъект персональных данных не в

[331] *Чжао Хун.* Обязательство государства защищать право на персональную информацию в контексте нового Гражданского кодекса // Обзор экономического и торгового права. 2021. № 2. С. 1-20.

состоянии конкурировать с ними.

В прошлом обработка персональных данных в основном была сосредоточена на известной личной информации, в то время как задача ее защиты заключалась в создании системы контроля, основанной на принципе информированного согласия. Однако, благодаря высокоразвитым технологиям обработки данных, объект обработки значительно выходит за рамки известной персональной информации. Персональная информация, полученная в результате анализа больших данных и использования искусственного интеллекта, затрагивает практически все аспекты субъекта информации[332], что с большой вероятностью может ущемить личностное достоинство человека. Поэтому при правовой защите персональных данных также следует уделять больше внимания контролю и регулированию технологических правил обработки данных, а не просто правовому регулированию обработки информации.

В-третьих, цель прямого закрепления в национальной конституции права на персональные данные заключается в восстановлении личностных прав и интересов, которыми люди должны пользоваться в ходе цифровой трансформации, а не в придании чрезмерного значения индивидуальным интересам при игнорировании потребностей общества в распространении информации и научно-техническом развитии. Именно в контексте появления тенденции чрезмерного контроля над природой человека по мере развития цифровых технологий родилось право на персональные данные. Суть защиты персональных данных заключается в уважении личности субъекта информации. С одной стороны, свободное развитие личности носит динамичный характер, но анализ технологий больших данных ограничен существующей информацией и привязан к прошлому. Человек не является ни данными, ни совокупностью электронных следов, однако технологии позволяют обрабатывать и интегрировать данные для формирования различных автоматизированных систем дифференциации, оценки, сортировки и принятия решений. Эти действия, в свою

[332] Чат-бот с искусственным интеллектом может генерировать информацию о пользователе на основе содержания разговора. URL: https://baijiahao.baidu.com/s?id=1779997946881942232&wfr=spider&for=pc (дата обращения: 20.11.2024).

очередь, делают наше «истинное я» неуместным на социальном уровне[333]. С другой стороны, чрезмерный сбор и анализ персональных данных с помощью цифровых технологий ограничивает пространство для свободного развития личности и ее автономии, а также может стать причиной злоупотребления государственной властью с целью наблюдения за отдельными лицами[334]. Защита персональных данных направлена на поддержание самостоятельности формирования личности и предотвращение навешивания ярлыков на личность в киберпространстве, препятствующих тем самым формированию и развитию личности.

Также важно учитывать, что существуют различия между правом на персональные данные и основными правами в области информатизации. Все основные права могут быть тесно интегрированы с правом на защиту персональных данных, закрепленным в конституционной доктрине в контексте процесса информатизации общества. Данное право, рассматриваемое как комплексное образование, обладает потенциалом эволюции и формируется в результате непрерывного развития технологий информатизации различных сфер жизни человека.[335] Иными словами, право на персональные данные представляет собой новое проявление всех существующих гражданских прав и законных интересов в условиях цифровой трансформации общества.[336]

Бесспорно, что право на персональные данные может быть связано со сферой защиты многих основных прав. При этом полагаем, что отрицание необходимости признания права на персональные данные в качестве независимого права является спорным. Наиболее обоснованными и логичными представляются следующие доводы:

Во-первых, выражение различных основных прав в сценарии информатизации по-прежнему является содержанием сферы защиты их прав, и

---

[333] *Чжэн Гэ.* Закон алгоритмов и алгоритм законов // Обзор законодательства Китая. 2018. № 2. С. 66-85.

[334] *Хун Данна.* Легитимность права забвения в эпоху больших данных // Журнал Южно-Китайского технологического университета. Общественные науки. 2021. № 1. С. 73-83.

[335] *Чжан Сян.* Конституционное подтверждение права на персональную информацию на основе размышления о теории разделения защиты и теории доминирования // Глобальный юридический обзор. 2022. № 1. С. 54-60.

[336] *Гао Фупин, Ли Цюньтао.* Новое позиционирование «прав и интересов в сфере персональной информации» в гражданском праве // Труды «Дунюэ». 2023. № 6. С. 166-176.

сфера защиты прав имеет мало общего с тем, включены ли они в сценарий информатизации. Хотя конкуренция между основными правами может возникать в силу различных сценариев, в целом сфера защиты основных прав в основном стабильна, а не меняется по мере изменения обстановки. Основные права в сценарии информатизации не обязательно выражаются в виде права на персональные данные. Более того, сама конкуренция основана на предпосылке различения более чем двух основных прав, то есть разница в объеме защиты прав является фундаментальной, но при определенных обстоятельствах могут быть пересечения. Таким образом, ключевой вопрос подтверждения права на персональные данные заключается не в сценарии информатизации, а в том, может ли существующая система защиты конституционных прав охватывать право на персональные данные, и на какие интересы охватывает сфера защиты прав на личную информацию.

Во-вторых, при пересечении между основными правами в сценарии информатизации и правом на персональные данные можно справиться с этим в соответствии с правилами конкуренции прав, однако те части прав, которые не пересекаются, фактически представляют различную сферу защиты, охватываемую разными основными правами. В соответствии с действующей системой защиты основных прав, закрепленной в Конституциях Китая и России, содержание права на персональные данные может быть относительно удовлетворительно отражено только путем расширенного толкования положения о человеческом достоинстве (Китай) или конституционных прав, таких как право на неприкосновенность частной жизни (Россия).

Права и интересы, связанные с персональными данными, значительно трансцендируют существующую систему конституционных прав. Право на персональные данные представляет собой самостоятельное фундаментальное право личности, которое эволюционировало в условиях цифровой трансформации и требует отдельного закрепления и защиты на конституционном уровне.[337]

[337] Ряд российских ученых также указывает, что право на защиту персональных данных является одной из разновидностей юридических гарантий конституционных прав человека. См.: *Вельдер И.А.* Система правовой защиты персональных данных в Европейском союзе: дис. ... канд. юрид. наук. Казань, 2006. С. 10; *Белгородцева*

Задачей информационного права является создание необходимых правовых условий для реализации данного права.

Важно также и то, что четкое установление права на персональные данные в конституции совместимо с атрибутами права на персональную информацию. В эпоху цифровых технологий национальные законодательные органы, с одной стороны, желают усилить конституционную защиту персональных данных, но, с другой стороны, обеспокоены тем, что чрезмерная их защита приведет к каким-нибудь непредвиденным последствиям.[338] Само по себе право на персональные данныепредставляет собой единство личных и общественных прав, что определяет сложный характер правовых благ от их защиты. Например, согласно статье 13 Закона КНР о защите персональной информации, в дополнение к получению личного согласия в качестве юридического основания для обработки персональных данных, операторы персональных данных могут также обрабатывать персональные данные при наличии определенных обстоятельств. Иными словами, в определенной ситуации больше не подчеркивается согласие субъектов персональных данных для обработки их личной информации, что в определенной степени ограничивает права и интересы физических лиц. Фактически, при обработке персональных данных в этих сценариях необходимо обеспечить баланс личных прав и общественных интересов, уделяя особое внимание потребностям общественного интереса. Так, разница в интенсивности защиты персональной информации обусловлена сложностью ее двойственных атрибутов: когда индивидуальные права и интересы не имеют преимущества в сравнении с общественными интересами, естественно, невозможно обеспечить их интенсивную защиту.

Таким образом, независимо от того, пытается ли кто-либо расширить сферу применения права на неприкосновенность частной жизни или расширить толкование личностных прав человека, трудно всесторонне справиться с

---

*Н.Г.* Теоретико-правовые аспекты защиты персональных данных: автореф. дис. ... канд. юрид. наук. М., 2012. С. 10–11, и др.

[338] *Пэн Чжунь.* Защита персональной информации с точки зрения Конституции: разъяснение характера, установление интенсивности и координация механизмов // Исследование о модернизации системы верховенства права. 2022. № 4. С. 50-64.

серьёзными угрозами обеспечения безопасности персональных данных в обществе информационных рисков [339]. Судя по последним изменениям в законодательстве о персональных данных в Китае и России, признание основных прав, присущих правам на персональные данные, является очень важной тенденцией[340]. Прямая конституционная защита прав на персональные данные может повысить эффективность, снизить возросшие издержки, связанные с толкованием применимых законов, и улучшить интеграцию правовой системы защиты личной информации. Следовательно, право на персональные данные следует позиционировать как новый тип права в рамках закрепленного в Конституции положения о человеческом достоинстве, а не присоединять его к существующим конституционным правам. Данное право в случае его законодательного закрепления на уровне Конституции может рассматриваться как фундаментальная публично-правовая мера обеспечения безопасности персональных данных, лежащая в основе других мер.

Вышеизложенное позволяет включить право на защиту персональных данных в систему конституционной защиты, что не только отвечает требованиям цифровой трансформации, но и может быть подтверждено теоретически. Безусловно, конституционный текст различных государств отличается относительной стабильностью, так что внесение поправок в конституцию непростая задача. Однако по мере того, как человечество движется к цифровому обществу, право на персональные данные как одно из прав человека нового поколения действительно требует четкой защиты со стороны Конституции, хотя для этого придется пройти долгий путь.

Таким образом, в рамках информационно-правового обеспечения безопасности персональных данных обоснованным представляется развитие концепции права на персональные данные как особого вида субъективных прав. При этом важно уточнить его соотношение с уже сформировавшимся в

---

[339] *Лю Цюань.* Различия в позиционировании права на защиту личной информации и их разрешение // Обзор законодательства Китая. 2022. № 6. С. 107-120.

[340] *Ши Цзяю.* Частноправовой аспект защиты личной информации: обсуждение взаимосвязи между Гражданским кодексом и Законом о защите персональной информации // Журнал сравнительного правоведения. 2021. № 5. С. 14-32.

российской доктрине и практике понятием «права на защиту персональных данных», производного от права на неприкосновенность частной жизни. Предлагаемая конструкция «права на персональные данные» рассматривается не как альтернатива, а как следующая ступень развития субъективных прав в контексте цифровой трансформации, смещающая акцент с пассивной «защиты» на активное правомочие по распоряжению и контролю над своими данными в рамках, установленных законом. Ценность данного подхода заключается в создании более гибкого и технологически нейтрального концептуального инструмента для механизма обеспечения безопасности персональных данных.

Во-первых, хотя абсолютный индивидуальный контроль над информацией (информационное самоопределение) не всегда соответствует природе информационного обмена, признание за субъектом определённого объёма правомочий по контролю и участию в процессах обработки его данных является необходимым. Во-вторых, данная концепция отличается гибкостью, позволяющей учитывать динамику современного развития технологий и обеспечивать защиту достоинства личности в новых условиях цифровой среды.

При формировании китайской и российской моделей информационного права определение места этого права в системе правоотношений влияет на создание целостного механизма защиты. В контексте системы субъективных прав в информационной сфере предлагается рассматривать право на персональные данные как правомочие, производное не только от охраны человеческого достоинства, но и от совокупности конституционных ценностей: неприкосновенности частной жизни, личной и семейной тайны, права на свободное развитие личности и защиты от произвольного вмешательства. Такой подход позволяет сбалансированно сочетать защиту прав субъектов данных с потребностями информационного общества, обеспечивая системное развитие информационного права.

## 3.2 Перспективы развития китайской и российской моделей публично-правового обеспечения безопасности персональных данных: сравнительный анализ

Сегодня персональные данные стали особо ценной информацией, значимой как для бизнеса,[341] так и развития государства в Китае и России. В этой связи важно рассмотреть перспективы развития основных публично-правовых моделей обеспечения безопасности персональных данных.

Рассмотрим в чем основное сходство и различие в публично-правовом обеспечении безопасности персональных данных в России и Китае в целях определения необходимости развития соответствующей российской и китайской моделей.

1) Понятие персональных данных и принципы их обработки в законодательстве Китая и России. Как выше было уже упомянуто, что специальное законодательство Китая и России четко определяет понятие персональных данных[342], т.е. в законодательстве обоих государств персональные данные определяются как информация, которая позволяет прямо или косвенно идентифицировать (определить) конкретное физическое лицо, то есть любая информация, связанная с идентифицируемым (определяемым) или уже идентифицированным (определенным) физическим лицом. Иными словами, законодательство об охране персональных данных в России и Китае четко регулирует категории информации, позволяющей осуществить идентификацию (определение) субъекта персональных данных. Таким образом, блага, связанные с персональными данными, находятся под защитой специального законодательства в обоих государствах. Только связь данных и личности по китайскому законодательству осуществляется через идентификацию, а по российскому

---

[341] *Гиш Т.А., Ржевская Н.В., Медведева А.С.* Анализ законодательства разных стран по обеспечению защиты персональных данных // Электронный научный журнал Курского государственного университета. 2023. № 4 (40). URL: https://api-mag.kursksu.ru/api/v1/get_pdf/5181/ (дата обращения: 31.12.2024).

[342] То есть, в статье 4 Закона КНР о ПДн и статье 3 Закона РФ о ПДн прямо установлена дефиниция персональных данных (персональной информации). Хотя термины и выражения, используемые в этих двух законах для определения персональных данных, не совпадают, значение персональных данных, выраженное в них, в основном одно и то же.

законодательству через определение субъекта. Использование термина «определенный», а не «идентифицируемый» в российском законодательстве происходит, потому что персональные данные – это всегда данные, относящиеся к конкретному лицу. ФЗ о ПДн также учитывает и информацию, которая может быть использована для идентификации, но не может быть использована для идентификации конкретного лица. Например, номер телефона может быть персональной информацией, если он позволяет идентифицировать пользователя, но не может быть использован для идентификации конкретного человека, если нет совокупности данных, таких как имя и номер телефона. Такой подход и помогает определить, какие данные являются персональными, а какие не являются, и обеспечивает защиту прав субъектов персональных данных. Поэтому не случайно мы ранее указывали, что китайский законодатель использует более общую категорию «персональная информация» и охраняет именно ее. Российский законодатель сужает в данном случае объект защиты и рассматривает персональные данные как специальную категорию, позволяющую четко определить в каждом конкретном случае конкретное физическое лицо.

В законодательстве КНР и РФ в сфере персональных данных, вслед за международными стандартами, устанавливается система принципов обработки персональных данных. В частности, статьи 5–9 Закона КНР о ПДн чётко формулируют пять ключевых принципов: законность, правомерность, необходимость и добросовестность; ограничение целей обработки; открытость и прозрачность; качество (целостность и точность); обеспечение безопасности. Следует отметить, что требование безопасности в Законе КНР о ПДн означает, что обработчик персональной информации должен принимать необходимые меры для обеспечения безопасности персональных данных. Этого рода требование также предусмотрено соответствующими законами и нормативными актами, такими как Решение ПК ВСНП об усилении защиты информации в интернете (в 2012 г.) и Закон КНР о кибербезопасности.

Согласно статье 5 ФЗ о ПДн, при обработке персональных данных должны соблюдаться следующие принципы: законность и справедливость (пункт 1);

соответствие заявленным целям обработки (пункты 2–5); точность, достаточность и актуальность (пункт 6); обязательное уничтожение или обезличивание данных после достижения целей их обработки (пункт 7). Кроме того, как мы указывали ранее, к принципам должен относиться и принцип обеспечения конфиденциальности (ст. 7 ФЗ о ПДн), который аналогичен принципу обеспечения безопасности в Китае.

Таким образом, специальное законодательство Китая и России в области персональных данных устанавливает принципы, которым необходимо следовать при обработке персональных данных. Эти принципы подчеркивают, что обработка должна осуществляться на законных основаниях, с четко определенной и разумной целью, ограничиваться минимально необходимыми действиями для достижения поставленной цели, проводиться в прозрачной форме, обеспечивать точность данных, предусматривать принятие мер безопасности и т.д. Кроме того, указанные принципы применимы ко всем этапам и аспектам обработки персональных данных.

2) Категории персональных данных в законодательстве Китая и России. Действующее российское законодательство предусматривает четыре категории обрабатываемых персональных данных: персональные данные общего режима; общедоступные; биометрические; специальные категории персональных данных. Несмотря на внесение различных изменений, четко прописаны только три первые группы, а вот в отношении последней нет конкретики.

Закон КНР о ПДн классифицирует персональные данные граждан на чувствительную [343] и обычную персональную информацию в соответствии с критериями бинарного разделения. Кроме того, Закон КНР о ПДн устанавливает правила защиты персональных данных умерших[344].

В целом законодательство Российской Федерации и Китайской Народной Республики обеспечивает правовую защиту любой персональной информации.

[343] Согласно ст. 28 к чувствительной информации относятся биометрические данные, сведения о религиозных убеждениях, особенностях личности, состоянии здоровья, финансовых счетах, местонахождении человека и другие данные, а также персональные данные о несовершеннолетних в возрасте до 14 лет.

[344] Конкретно, ст. 49 касается обращения, связанного с информацией, оставшейся в интернете после смерти физического лица в эпоху больших данных.

Основное различие между ними состоит в том, что персональные данные делятся либо на четыре категории, либо на две. Представляется, что классификация персональных данных в соответствии с российским законодательством о персональных данных является чрезмерно детализированной. Например, биометрическая информация и специальная информация в определенных сценариях абсолютно могут быть отнесены к чувствительным персональным данным[345].

В Законе КНР о ПДн персональные данные делятся на чувствительную и нечувствительную личную информацию, а также на этой основе определяются специальные правила обработки чувствительной персональной информации, что соответствует тенденциям развития законодательства о персональных данных в большинстве государств мира и позволяет более эффективно предотвращать риски, связанные с персональной информацией. В то же время различение двух типов персональных данных может повысить предсказуемость процесса обработки, прояснить направленность корпоративного комплаенса и в определенной степени снизить затраты на соблюдение корпоративного комплаенса, что способствует развитию цифровой экономики. Тем не менее, существует ряд сложностей, связанных с определением и защитой чувствительной личной информации, поскольку её характеристики носят ситуативный характер, а сама информация может быть признана чувствительной не только исходя из её содержания, но и в зависимости от конкретного сценария (цели) ее использования и совершения иных действий.[346] Рассмотрим эти проблемные вопросы.

***Определение чувствительной личной информации.*** В условиях цифровой среды и активного использования цифровых технологий возникает всё больше неопределённостей при определении категории чувствительной личной информации. Благодаря технологиям, в том числе веб-поиску, пользователи получают доступ к значительному объёму открытых персональных данных и

[345] *Ван Гуанлун.* Административно-правовые меры по обеспечению безопасности персональных данных при раскрытии информации правительством в Китае // Вестник Санкт-Петербургского университета. Право. 2024. № 3. С. 815-834.

[346] См.: *Дин Сяодун.* Пояснительная реконструкция системы защиты конфиденциальной личной информации // Юридическая наука в Китае. 2025. № 2. С. 168.

связанных с ними справочных сведений. Комбинируя эти данные с другими источниками информации, соответствующие субъекты могут преобразовать их в информацию, относящуюся к категории чувствительных личных данных.

Например, в скандальном инциденте с компанией Cambridge Analytica[347] данная организация изначально собирала преимущественно нечувствительные персональные данные физических лиц. Тем не менее, благодаря агрегированию и проведению анализа больших данных, в конечном итоге удалось получить значительный объем чувствительной личной информации, включая такие параметры, как политические предпочтения отдельных индивидуумов. С учетом развития информационных технологий и расширения масштабов аналитической индустрии можно прогнозировать, что процесс вывода чувствительной личной информации из нечувствительных данных станет более частым явлением.

Причина, по которой определённые типы персональных данных считаются чувствительными, заключается в том, что такие данные затрагивают важнейшие права и интересы личности. Несоблюдение требований к их обработке или защите может привести к серьёзным рискам для индивидуума. В зависимости от разных сценариев риски, связанные с обработкой различных типов персональных данных, могут значительно различаться, что делает определение категории «чувствительная личная информация» зависимым от множества факторов. При классификации персональной информации как чувствительной необходимо учитывать следующие аспекты.

Во-первых, степень чувствительности личной информации должна оцениваться с учётом индивидуальных характеристик субъекта данных. Сведения о лицах, которые не обладают достаточными возможностями для самостоятельной защиты от потенциальных рисков, целесообразно относить к информации повышенной чувствительности. К числу наиболее типичных примеров относятся персональные данные несовершеннолетних. Особенности их психического развития и отсутствие полностью сформированной самостоятельной воли

---

[347] См.: Прошлое и настоящее «шокирующего скандала» с компанией Cambridge Analytica. URL: https://news.sina.cn/global/szzx/doc-ifyspkni4321306.d.html?cid=57929&oid=5_hn163 (дата обращения: 12.05.2025).

обусловливают необходимость более строгого подхода к обработке таких данных.[348] В ряде ситуаций пожилые люди также могут рассматриваться как уязвимая категория субъектов персональных данных, поскольку риск использования их информации в мошеннических целях является повышенным. Так, получение злоумышленниками контактных данных пожилого человека в сочетании с иными достоверными сведениями может создать условия для совершения телекоммуникационного или интернет-мошенничества. Кроме того, более осторожного режима обработки требуют сведения о лицах с ограниченными физическими возможностями и иных группах, подверженных социальному неравенству и дискриминации. Информация, раскрывающая принадлежность лица к таким группам, должна квалифицироваться как чувствительная персональная информация.

Во-вторых, чувствительность персональной информации должна оцениваться с учётом субъекта, осуществляющего её обработку. Степень чувствительности данных зависит не только от их содержания, но и от статуса оператора, целей обработки и применяемых методов идентификации. Например, для крупной организации, использующей автоматизированную обработку, сведения о домашнем адресе или месте работы сотрудника могут не рассматриваться как данные повышенной чувствительности при наличии надёжных механизмов шифрования, обезличивания и ограничения доступа. Вместе с тем для самого субъекта персональных данных раскрытие такой информации может повлечь риски для личной безопасности, благополучия и безопасности членов его семьи. В связи с этим оценка чувствительности должна учитывать не только меры, принимаемые оператором, но и характер возможных последствий для лица, а также особенности обработки данных государственными и негосударственными организациями. Указанные различия связаны с особенностями обработки данных, различным уровнем их защищённости, а также с характером потенциальных

[348] См.: *Чжан Сухуа, Инь Сяокунь.* Теоретические основы и оценка способности несовершеннолетних давать согласие на персональных данные // Финансовое и экономическое право. 2023. № 6. С. 3-17.

рисков нарушения прав субъектов персональных данных.[349]

В-третьих, оценка чувствительности персональной информации должна учитывать способ её обработки. Значение имеет не только содержание самих данных, но и то, каким образом они собираются, анализируются, сопоставляются с иными сведениями и используются для идентификации лица. В данном контексте Рональд Лайнс предлагает различать несколько типов идентификации[350]:

- идентификация L-типа, или поисковая идентификация, направлена на установление конкретного лица. Она осуществляется с использованием таких идентификаторов, как имя, номер телефона, номер паспорта и иные сведения, позволяющие найти определённого человека;

- идентификация R-типа（recognition）, используется для подтверждения личности пользователя. Например, при банковском обслуживании такая идентификация может осуществляться с применением технологии распознавания лица клиента;

- классификация C-типа (classification) используется для распределения лиц по определённым категориям, например по признаку расовой принадлежности или принадлежности к конкретной группе потребителей;

- идентификация S-типа (session) предназначена для обеспечения взаимодействия и обмена данными в рамках конкретного пользовательского сеанса. Так, веб-сайты могут использовать файлы cookie для сохранения информации о товарах, добавленных пользователем в корзину, что позволяет системе распознавать состояние сеанса и обеспечивать переход к последующим этапам оформления заказа.

Чувствительность личной информации следует оценивать с учётом того, какой тип идентификации применяется в конкретной ситуации. Например, использование идентификаторов L-типа, включая номера удостоверений личности

---

[349] См.: *Чжао Хун.* Применение и ограничения уведомления и согласия при исполнении государственных обязанностей // Глобальный юридический обзор. 2022. № 2. С. 36-51.

[350] See Ronald Leenes, Do They Know Me? Deconstructing Identifiability, University of Ottawa Law & Technology Journal, Vol.4:135, p.148 (2007).

и паспортов, позволяет однозначно установить конкретное лицо. В таком случае соответствующие сведения должны рассматриваться как чувствительная личная информация. Иная ситуация складывается при применении идентификации C- или S-типа: сами по себе номера удостоверений личности и паспортов не всегда относятся к чувствительным данным и не обеспечивают прямого установления личности. Вместе с тем отдельные категории идентификационной информации, такие как расовое происхождение, политические взгляды, религиозные или философские убеждения, при C-классификации могут использоваться для выделения определённых групп лиц, что создаёт риск дискриминации. При использовании иных способов идентификации чувствительность этих сведений может быть ниже, поскольку они не позволяют однозначно определить конкретного человека.

В-четвёртых, при отнесении информации к чувствительным персональным данным следует учитывать вероятность идентификации конкретного лица на её основе. Даже если после сбора такие сведения подвергаются шифрованию или обезличиванию, это не всегда исключает возможность последующего установления личности. Информация может сохранять персональный характер, если она позволяет косвенно идентифицировать человека либо установить его связь с иными конкретными данными. Поэтому с позиции защиты прав субъектов персональных данных степень идентификационного потенциала информации является одним из ключевых критериев её чувствительности. [351] Степень чувствительности персональных данных во многом зависит от вероятности идентификации физического лица в процессе их обработки. При высокой вероятности установления личности такие данные следует относить к категории повышенной чувствительности, тогда как при низком идентификационном потенциале уровень чувствительности может быть признан сравнительно невысоким.[352]

---

[351] See Sophie Stalla-Bourdillon & Alison Knight, Anonymous Data v. Personal Data - A False Debate: An EU Perspective on Anonymisation, Pseudonymisation and Personal Data, Wisconsin International Law Journal, Vol.34:284, p. 284-322 (2017).

[352] См.: *Лю Сяочунь.* Разработка правил защиты и использования общедоступной личной информации // Глобальный юридический обзор. 2022. № 2. С. 52-68.

Следует отметить, что чувствительность личной информации определяется с учётом конкретного сценария её обработки. В связи с этим основания для её оценки не исчерпываются указанными выше факторами и могут включать дополнительные критерии, отражающие особенности соответствующих правоотношений:

- при отнесении информации к категории чувствительной личной информации следует учитывать три ключевых обстоятельства: потенциальный вред, который может возникнуть в результате её утечки, вероятность наступления неблагоприятных последствий для субъекта персональных данных, а также степень общественного восприятия конкретного вида информации как чувствительного;[353]

- идентификация чувствительных личных данных должна осуществляться путём объединения статической модели оценки, основанной на критериях «последствия ущерба» и «общие ожидания конфиденциальности», с динамической сценарной моделью, в которой наряду с указанными критериями учитывается также «цель использования» информации;[354]

- при оценке чувствительности личной информации необходимо учитывать тяжесть потенциального ущерба, вероятность его возникновения, степень общественного признания такой информации как чувствительной, а также возможность технического прогнозирования связанных с ней рисков;[355]

- при оценке чувствительности личных данных необходимо учитывать содержание информации, контекст её использования и иных действий с ней, степень её инструментальной значимости и потенциал уникальной идентификации. Кроме того, значение имеют когнитивные и технические возможности субъекта обработки, его способность использовать полученные

---

[353] См.: *Ху Вэньтао.* Концепция определения чувствительной личной информации в Китае // Юридическая наука в Китае. 2018 № 5. С. 235-254.
[354] См.: *Су Чэнхуэй.* Об ограничении доступа к транзакционным данным // Современное право. 2020. № 5. С. 147.
[355] См.: *Се Линь, Ван Сюань.* Содержание и объем чувствительной личной информации в Китае // Электронная интеллектуальная собственность. 2020. № 9. С. 4-16.

сведения, а также правовой и фактический статус субъекта данных;[356]

- отнесение информации к категории чувствительной личной информации должно осуществляться не абстрактно, а с учётом конкретного контекста обработки. Для этого необходимо комплексно оценивать пять элементов: субъекта личной информации, обработчика данных, третье лицо, характер информации и цель её обработки.[357]

Каждая из рассмотренных позиций формулирует самостоятельные критерии оценки чувствительной личной информации и дополняет представление о её специфике в зависимости от контекста обработки, целей использования и иных действий с такими данными.[358]

Таким образом, перечисленные факторы позволяют более обоснованно оценивать, относится ли тот или иной вид личной информации к категории чувствительной с учётом конкретного сценария её обработки. При этом они не предназначены для однозначного определения того, относится ли конкретный тип личной информации к категории чувствительной. Это объясняется тем, что степень чувствительности личной информации зависит не от её внутренних характеристик, а от специфики и условий конкретного сценария (цели) её использования и совершения иных действий.

**Способы защиты чувствительной личной информации.** Для адаптации к характеристикам определения чувствительной личной информации, основанным на сценариях, в административном надзоре в Китае рекомендуется применять сценарный подход к защите данных. Такой подход предполагает внедрение мер безопасности снизу вверх, опираясь на соответствующие правовые толкования, административные регламенты и нормативные акты.

Такой подход к защите обусловлен необходимостью избегать универсального

---

[356] См.: *Нинь Юань.* Правовые стандарты и определение сферы чувствительной личной информации в Китае: на примере пункта 1 статьи 28 Закона КНР о защите персональной информации // Журнал сравнительного правоведения. 2021. № 5. С. 33-49.

[357] См.: *Ван Юань.* Концептуальное определение и оценка элементов чувствительной личной информации: на примере статьи 28 Закона о КНР защите персональной информации // Глобальный юридический обзор. 2022. № 2. С. 85-99.

[358] См.: *Чжэн Цзэсин.* Об охране правовых благах от преступления в нарушении персональной информации граждан: теоретическая структура и практическая позиция контекстуализированных правовых благ // Цинхуаское право. 2023. № 3. С. 90-105.

усиления защиты чувствительной личной информации на высоком уровне законодательства. Вместо закрепления единого и исчерпывающего перечня чувствительной личной информации более обоснованным представляется определение её категорий с учётом конкретных сфер деятельности и сценариев обработки данных. Соответствующие критерии могут устанавливаться в профессиональных стандартах, отраслевых правилах и специальных нормативных требованиях. Такой подход особенно актуален для отраслей и подсекторов, в которых сходные бизнес-модели обусловливают близость методов сбора данных, их использования, хранения и защиты, а также рисков утечки и последующего неправомерного использования информации. Поэтому дифференцированная защита персональных данных должна формироваться применительно к каждой отрасли или подсектору с учётом уровня чувствительности соответствующей информации. При этом специальные отраслевые стандарты обладают большей гибкостью и могут быстрее адаптироваться к изменению технологических и организационных условий. Различные типы персональной информации могут быть динамически скорректированы для обеспечения адекватной защиты в зависимости от связанных с ней рисков [359], что позволяет минимизировать проблемы задержки или несогласованности, возникающие после принятия законов и нормативных правовых актов высокого уровня.

Таким образом, в качестве системного инструмента для классифицированной и дифференцированной защиты личных данных единое определение и специальная защита чувствительной личной информации были закреплены на законодательном уровне большинством государств и регионов. Основная цель защиты личных данных заключается в обеспечении соответствующих прав и интересов субъектов данных, а также в минимизации рисков, возникающих при их использовании в конкретных ситуациях. Защита не ограничивается самими данными, а фокусируется на предотвращении негативных последствий их использования и совершения иных действий. Таким образом, степень

[359] См.: *Су Юй, Гао Вэньин.* Стандарты идентификации личной информации: источник, практика и размышления // Право Шанхайского университета транспорта. 2019. № 4. С. 54-71.

чувствительности персональных данных должна оцениваться исключительно в зависимости от конкретного сценария применения, а не может оставаться неизменной или оцениваться по самим персональным данным.

**Гарантии обеспечения безопасности персональных данных в Китае и России.** Они заключаются в следующем:

а) Четкое законодательное закрепление прав граждан на персональные данные в Законе КНР о ПДн (в статьях 46, 47) и ФЗ о ПДн (в главе 3). Разница заключается в том, что в Китае помимо Закона КНР о ПДн существует ряд других специальных нормативных правовых актов, которые также предусматривают права на персональные данные, например, в Законе КНР «О кибербезопасности», Положении КНР о защите персональной информации пользователей телекоммуникаций и Интернета и др[360].

б) Обязанности операторов в процессе обработки персональных данных. Так, в главе 4 ФЗ о ПДн предусмотрено достаточно много обязанностей оператора персональных данных. В свою очередь, Закон КНР о ПДн в главе 5 также предусматривает ряд обязанностей оператора при обработке персональных данных.

в) Определение органов для осуществления функции по защите персональных данных. Государственные органы для осуществления функции по защите персональных данных и соответствующая ответственность за их нарушение требований закона, прямо предусмотрены в главах 6, 7 Закона КНР о ПДн, и в главе 5 ФЗ о ПДн. В России основным органом выступает Роскомнадзор [361] ; в Китае таким органом являются Государственная администрация по киберпространству и соответствующие органы исполнительной

---

[360] *Ван Гуанлун.* Административно-правовая защита персональной информации в Китае: недостатки и путь решения // Вестник Университета имени О.Е. Кутафина (МГЮА). 2024. № 10. С. 189-197.

[361] К полномочиям Роскомнадзора относится осуществление федерального государственного контроля (надзора) за обработкой персональных данных, обращение в суд с исковыми заявлениями в защиту прав субъектов персональных данных и неопределенного круга лиц, привлечение к административной ответственности лиц, виновных в нарушении Федерального закона "О персональных данных", рассмотрение жалоб и обращений по вопросам, связанным с обработкой персональных данных, ведение реестра операторов, осуществляющих обработку персональных данных, ограничение доступа к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных. См.: на вопросы в сфере защиты прав субъектов персональных данных. https://sudact.ru/law/informatsiia-roskomnadzora-otvety-na-voprosy-v-sfere_1/ (дата обращения: 30.12.2024).

власти (отделы), выполняющие обязанности по защите персональной информации (ст. 60 Закона КНР о ПДн). Следовательно, в России Роскомнадзор выступает в качестве специального уполномоченного органа по регулированию защиты персональных данных[362]. В Китае такие функции регулирования сосредоточены в Государственной администрации по киберпространству, при этом так называемые специализированные органы для осуществления обязанностей по защите персональных данных остаются не четко определенными.

4) Требования к трансграничной передаче персональных данных[363] в Китае и России. В главе 3 Закона КНР о ПДн специально предусмотрены правила трансграничного предоставления персональных данных[364]. В соответствии с положениями ФЗ о ПДн, в частности п. 11 ст. 3 и ч. 5 ст. 12, трансграничная передача персональных данных допускается только при условии получения оператором необходимых сведений от соответствующих иностранных получателей и представления такой информации по требованию Роскомнадзора. Детальная регламентация данного процесса закреплена в Постановлении Правительства РФ от 10.01.2023 № 6[365], которое устанавливает исчерпывающие критерии оценки соответствия уровня защиты персональных данных в стране-реципиенте, включая оценку адекватности правового режима защиты данных, наличия эффективных средств правовой защиты и соблюдения международных обязательств. Указанный нормативный акт также определяет процедуру принятия решений уполномоченным органом, предусматривающую проведение комплексного анализа рисков и уведомление операторов о введенных ограничениях в трехдневный срок, что создает сбалансированный механизм

---

[362] *Ван Гуанлун.* Административно-правовая защита персональной информации в Китае: недостатки и путь решения // Вестник Университета имени О.Е. Кутафина (МГЮА). 2024. № 10. С. 189-197.

[363] Трансграничная передача персональных данных – это передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

[364] Например, «Без разрешения компетентного органа Китайской Народной Республики оператор персональной информации не должен предоставлять персональную информацию, хранящуюся на территории Китайской Народной Республики, судебным или правоохранительным органам за пределами территории Китайской Народной Республики» (ст. 41).

[365] Постановление Правительства РФ от 10.01.2023 № 6 «Об утверждении Правил принятия решения о запрещении или об ограничении трансграничной передачи персональных данных уполномоченным органом по защите прав субъектов персональных данных и информирования операторов о принятом решении» // Справочная правовая система «Консультант Плюс».

защиты прав субъектов персональных данных при обеспечении национальных интересов в цифровом пространстве.

На основе проведенного сравнительно-правового исследования в сфере защиты персональных данных в России и Китае можно констатировать наличие общих правовых проблем и перспективных направлений для дальнейшего научного изучения данного вопроса. Вместе с тем, представляется затруднительным однозначно оценить, какая правовая система – российская или китайская – демонстрирует более высокий уровень целостности в обеспечении защиты персональных данных, поскольку каждое государство характеризуется уникальным подходом к регулированию обработки персональных данных и их защите.

В целом законодательство, регулирующее обработку персональных данных в России и Китае, имеет как сходства, так и различия. С точки зрения сходства везде законодательно установлено, что операторы должны получать согласие от отдельных физических лиц (субъектов персональных данных), прежде чем собирать их личные данные, и обязывают принимать соответствующие меры безопасности для защиты данных. Кроме того, в обоих государствах приняты законы, обеспечивающие безопасность персональных данных.

Однако есть и некоторые отличия. Например, законодательство Китая предоставляет физическим лицам более широкий спектр отдельно выделенных прав в области обеспечения безопасности персональных данных по сравнению с российским. В частности, Закон КНР о персональных данных прямо закрепляет за субъектами права на удаление и переносимость данных, а также возлагает на операторов обязанность уведомлять заинтересованных лиц и уполномоченный орган о случаях утечки или утраты персональной информации. В российском регулировании сходные возможности также присутствуют, однако они реализуются преимущественно через системное толкование норм и принципов обработки персональных данных либо через специальные правовые институты. Отдельное различие проявляется в регулировании биометрических данных. Так,

Постановление Правительства РФ от 16.06.2022 № 1089 [366] предусматривает создание централизованной системы обработки биометрической информации, что отражает приоритет инфраструктурного подхода над расширением индивидуальных правомочий субъектов данных. Указанный акт устанавливает технические и организационные требования к единой биометрической системе, включая процедуры верификации и проверки соответствия биометрических показателей, однако не вводит дополнительных гарантий для субъектов персональных данных. Такой подход отражает специфику российской модели защиты персональных данных, где акцент смещен в сторону создания централизованных систем управления данными при относительной ограниченности индивидуальных контрольных механизмов.

Еще одно ключевое отличие – требование к операторам хранить персональные данные внутри государства. Россия обязывает хранить персональные данные на своей территории, тогда как в Китае такого требования нет.

На основе вышесказанного сходства и различия можно представить в виде специальной таблицы.( Приложение 2 )

**2. Сравнительный анализ административных санкций за нарушение законодательства о персональных данных в Китае и России**

1) В Китае положения об административной ответственности за нарушение прав и интересов, связанных с персональными данными, закреплены в Законе КНР о ПДн, Законе КНР о кибербезопасности, Законе КНР о наказаниях за нарушение общественного порядка и Законе КНР об административных наказаниях. В частности, в последних законах содержатся общие нормы об административных санкциях.

Закон КНР о ПДн в отдельной седьмой главе детально регламентирует юридическую ответственность, включая административную, за нарушение правил

[366] Постановление Правительства РФ от 16.06.2022 № 1089 «Об утверждении Положения о единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица» // Собрание законодательства РФ. 2022. № 26. Ст. 4163.

обработки персональных данных. Причем, кроме статьи 69, регламентирующей гражданскую ответственность, в остальных статьях (ст.ст. 66-68, 70-71) этого закона предусмотрена административная ответственность разных субъектов в различных обстоятельствах, что заключается в следующем:

а) внесение записей в кредитный архив за нарушения любого из требований, предусмотренных в Законе КНР о ПДн (ст. 67)[367].

б) в отношении негосударственных операторов применяется обязательное исправление с вынесением предупреждения, конфискацией незаконных доходов либо приостановлением или прекращением предоставления услуг приложением за нарушение персональных данных без отягчающих обстоятельств; за отказ от исправления - штраф в размере до 1 млн юаней; в отношении непосредственно ответственных лиц и других конкретных ответственных лиц - наложение штрафа в размере от 10 до 100 тыс. юаней (ч. 1 ст. 66); за совершение такого рода правонарушения с отягчающими обстоятельствами – обязательное исправление с конфискацией незаконных доходов, штрафом в размере до 50 млн юаней или до 5% от оборота за предыдущий год, а также с приостановлением ведения бизнеса или приостановлением бизнеса для исправления либо уведомлением об отказе указанного разрешения на ведение бизнеса или отзыве лицензии в компетентные ведомства  или без такового; к непосредственно ответственным лицам или другим конкретным ответственным лицам  применяется наложение штрафа в размере от 100 тыс. до 1 млн юаней, а к соответствующим должностным лицам – лишение их права занимать свою должность (ст. 2 ст. 66).

в) в отношении государственных органов в качестве операторов применяется требование к исправлению и привлечение непосредственно ответственных лиц и других конкретных ответственных лиц к дисциплинарной или административной ответственности за их правонарушения.

Статья 64[368] и статья 44[369] Закона КНР о кибербезопасности специально

[367] Статья 67 Закона КНР о ПДн: Любое противоправное действие, указанное в настоящем Законе, должно быть зарегистрировано в кредитные архивы в соответствии с положениями соответствующих законов и административных правил и должно быть обнародовано.

[368] Так, статья 64 указанного закона гласит: «Нарушение сетевыми операторами и поставщиками сетевых продуктов или услуг пункта 3 статьи 22 или статей 41–43 настоящего закона …… может независимо или

предусматривают административную ответственность за нарушение законодательства о защите персональных данных.

2) Согласно статье 24 ФЗ о ПДн[370], несоблюдение требований относительно обработки персональных данных предполагает привлечение к различным видам ответственности, причем наказать могут как уполномоченного за безопасность информации сотрудника, так и все предприятие.

Так, за нарушения требований, предусмотренных ФЗ о ПДн, с учетом конкретных обстоятельств и серьёзности деяния могут грозить разные виды административной ответственности, закрепленные в КоАП РФ.

Как известно, в ноябре 2024 года, в России появился новые изменения и дополнения к статьям 13.11 и 13.11.3 Кодекса РФ об административных правонарушениях (далее – КоАП РФ), предусмотренные Федеральным законом № 420 «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» (далее – Закон № 420-ФЗ)[371]:

а) Изменения в ст. 13.11 КоАП, внесенные Законом № 420-ФЗ, отражаются в таких аспектах, как:

- увеличение размеров административных штрафов за обработку персональных данных в определенных случаях;

- дополнение ряда новых видов административных правонарушений и соответствующей ответственности за них;

- ужесточение ответственности за правонарушения в виде неправомерной передачи персональных данных;

---

одновременно повлечь за собой предупреждения, конфискацию незаконного дохода и/или штраф в 1–10-кратном размере незаконных доходов; при отсутствии незаконных доходов взимается штраф до 1 млн юаней, …».

[369] Нарушение статьи 44 настоящего закона путем кражи или использования других незаконных средств для получения, незаконной продажи или незаконного предоставления другим личной информации, если не является преступлением, влечет за собой конфискацию незаконных доходов органами общественной безопасности и штраф в 1–10-кратном размере незаконных доходов, а при отсутствии незаконных доходов взимается штраф до 1 млн юаней».

[370] Статья 24 Закона РФ о ПДн: «Лица, виновные в нарушении требований настоящего Федерального закона, несут предусмотренную законодательством Российской Федерации ответственность»

[371] Указанный закон вступает в силу 30 мая 2025 г. Большинство положений Закона № 420-ФЗ посвящены дальней шей диверсификации видов правонарушений и ужесточению административной ответственности в сфере законода тельства РФ о персональных данных. Указанная диверсификация и ужесточение административной ответственност и в основном отражается в следующем. См.: Обзор изменений законодательства: ужесточение ответственности за н арушение законодательства о персональных данных. URL: https://www.unicon.ru/insights/obzor-izmenenii-zakonodate lstva/Tougher_liability_for_violations_of_the_law_on_personal_data/ (дата обращения: 30.12.2024).

- введение административной ответственности за деяния операторов, повлекшие неправомерную передачу специальных персональных данных и биометрических персональных данных;

- ужесточение ответственности в отношении лиц, подвергнутых административному наказанию за отдельные нарушения.

б) Изменения и дополнения в ст. 13.11.3 КоАП[372], внесенные Законом № 420-ФЗ, заключаются в дополнении новых частей 2, 3 в ст. 13.11.3[373]. Основное содержание этих добавленных новых частей проявляется в следующем:

- в части 2 предусмотрена административная ответственность за нарушение порядка обработки биометрических персональных данных в определенных областях;

- часть 3 касается административной ответственности за неприятие определенных мер, связанных с обеспечением безопасности биометрических персональных данных;

- введение ответственности за обработку за нарушение порядка обработки биометрических персональных данных в определенных областях.

Начиная с 30 мая 2025 года, согласно статье 13.11 КоАП РФ, размер штрафов для индивидуальных предприятий и компаний увеличится и будет зависеть от количества людей, чьи персональные данные подверглись утечке. Таким образом, в российском законодательстве прослеживается четкая тенденция к ужесточению ответственности за нарушения законодательства о персональных данных и дальнейшему разнообразию составов административных правонарушений. В связи с этим, чтобы избежать рисков административных взысканий, операторам персональных данных необходимо, по крайней мере, обеспечить полное соблюдение ими соответствующих законов и нормативных актов, а также обеспечить безопасность данных в используемых ими информационных

[372] В новой редакции статьи речь идет о нарушении законодательных требований в области размещения и обработки биометрических персональных данных в государственной информационной системе «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных» и иных информационных системах, обеспечивающих аутентификацию на основе биометрических персональных данных.

[373] Ст. 13.11.3 КоАП дополнена новыми частями 2, 3 и 4. В отличие от ст. 13.11 КоАП, здесь субъектами нарушений являются только должностные лица и юридические лица, а распространяется статья в основном на деятельность государственных органов, Банка России и иных специализированных организаций.

системах[374].

3) Сравнительный анализ мер административного наказания за нарушение законодательства о персональных данных в Китае и России. Вышеизложенное сравнение показывает, что существенные различия между мерами административного наказания, предусмотренными в законодательстве Китая и России, в основном отражаются в следующих моментах.

а) Различия в законодательной модели административной ответственности. При сравнении законодательной модели административной ответственности за нарушение персональных данных в России и Китае видно, что в ФЗ о ПДн предусмотрены типичные правонарушения в сфере персональных данных и в отдельных статьях КоАП РФ закреплены соответствующие конкретные административные наказания за указанные правонарушения. В Законе КНР о ПДн регламентированы не только правонарушения в сфере защиты личной информации, но и в отдельных статьях этого закона (ст.ст. 66, 67) предусмотрены конкретные меры административного наказания за указанные правонарушения. Кроме того, в Законе КНР о кибербезопасности, вступившем в силу 1 июня 2017 года, также содержится отдельная статья (ст. 64), предусматривающая конкретные меры административного наказания за незаконное получение, использование, незаконную продажу и незаконное предоставление личной информации.

б) Различия в субъектах, обращающихся в суд за защитой нарушенных прав на персональные данные. В Китае – это сами субъекты персональных данных, Народная прокуратура, определенные законом организации потребителей или организации, определенные Государственной администрацией по киберпространству. В России – это субъекты персональных данных, Роскомнадзор, прокуратура.

в) Виды административных наказаний в Китае и России достаточно различаются. Согласно КоАП РФ, правонарушителей в сфере персональных данных могут наказывать предупреждением или административным штрафом. В

[374] Новые штрафы за утечку персональных данных и другие нарушения при работе с ними: закон опубликован. URL: https://www.consultant.ru/legalnews/27142/?ysclid=maafdpkrk0907274021 (дата обращения: 30.02.2025).

Китае в отношении этого рода нарушителей применяются такие виды административных наказаний, как: предупреждение, конфискация незаконных доходов, административный штраф, запрет занимать определенные должности в определенный срок (ст. 66 Закона КНР о ПДн), а также административный арест, предусмотренный статьей 71 Закона КНР о ПДн, Законом КНР о наказаниях за нарушение общественного порядка и Законом КНР об административных наказаниях[375].

г) Размер административных штрафов, предусмотренных законами Китая и России, значительно отличается. Китайское законодательство предусматривает три вида административных штрафов: штрафы, кратные размеру незаконных доходов (ст. 64 Закона КНР о кибербезопасности); штрафы в процентах от оборота (ч. 2 ст. 66 Закона КНР о ПДн); простые штрафы. В статьях КоАП РФ об административных наказаниях за правонарушения в сфере персональных данных до 30 мая 2025 г. предусматриваются лишь простые штрафы, а Законом № 420-ФЗ внесены оборотные штрафы.

Таким образом, по результатам исследования предложен новый системный подход к категоризации персональных данных в Китайской Народной Республике, основанный на динамической, контекстуально-зависимой оценке их чувствительности. Установлено, что степень чувствительности личной информации зависит не только от её внутренних характеристик, а также от специфики и условий конкретного сценария (цели) её использования и совершения иных действий. Основная цель обеспечения безопасности персональных данных заключается в гарантировании защищенности прав и законных интересов субъектов персональных данных, в минимизации рисков, связанных с их использованием и совершением иных действий с ними, в том числе на предотвращении возможных негативных последствий таких действий, а также в восстановлении нарушенных прав. Для адаптации к особенностям определения чувствительной личной информации, основанного на контексте

---

[375] *Ван Гуанлун.* Механизм административно-правового регулирования защиты персональных данных в Китае: состояние, недостатки и путь решения. // Вестник Московского университета. 2024. Серия 11. Право. Том 65. № 4. С. 204-232.

конкретных сценариев (целей), рекомендуется внедрение разработанного системного подхода к обеспечению безопасности данных, подразумевающего внедрение публично-правовых мер, основанных на соответствующих правовых толкованиях, административных регламентах и отраслевых правилах. Выявлено, что такая динамическая дифференциация способствует повышению предсказуемости и эффективности обработки данных, оптимизации корпоративного комплаенса и связанных с ним затрат, что, в свою очередь, создает благоприятные условия для развития экономики данных.

Установлено, что подход к категорированию персональных данных, установленный в Российской Федерации, учитывая особенности обработки и защиты персональных данных, в целом отвечает требованиям публично-правового обеспечения их безопасности. В сравнительном аспекте отмечено, что выделение в Российской Федерации биометрических персональных данных в отдельную категорию, обособленную от специальных категорий персональных данных, создаёт дополнительные сложности в правоприменении и административные барьеры, не всегда соотносимые с гибкостью риск-ориентированного подхода.

## 3.3 Основные направления совершенствования публично-правового обеспечения безопасности персональных данных в Китае и России

### 1. Необходимость совершенствования публично-правового обеспечения безопасности персональных данных в современных условиях

Вступление эры больших данных оказало мощное влияние на развитие человеческого общества. Преобразуя способы информационного взаимодействия и повышая эффективность социальных процессов, данная технологическая революция также порождает управленческие проблемы, которые требуют решения.

Большие данные основаны на инфраструктуре Интернета и новых цифровых технологий. Удобство получения информации и универсальность доступа к ней представляют собой два аспекта диалектического единства: с одной стороны,

современные цифровые технологии позволяют преодолеть временные и пространственные ограничения для достижения свободы обмена информацией; с другой стороны, широкое распространение механизмов сбора и обработки данных ставит граждан в дилемму цифрового выживания в виде «паноптического наблюдения»[376].

Это превращает обеспечение безопасности персональных данных в одну из ключевых задач управления в ходе цифровой трансформации. С бурным развитием цифровой экономики персональные данные приобрели значительные имущественные свойства, что требует от системы правовой защиты создания специальных мер публично-правового обеспечения безопасности персональных данных. По сравнению с мерами защиты в связи с привлечением к административной ответственности после совершения правонарушений и уголовными санкциями, в которых особое внимание уделяется строгому противодействию, механизм публично-правового обеспечения безопасности персональных данных, направленный прежде всего на превенцию нарушений в данной сфере, обладает уникальными институциональными преимуществами.

1) Преимущества комплексной публично-правовой системы обеспечения безопасности персональных данных. Нарушение прав и законных интересов в сфере персональных данных может происходить как со стороны государства, так и со стороны других субъектов обработки персональных данных, причем значительная часть нарушителей представляет собой государственные и муниципальные органы. Возможности физических лиц по защите своей личной информации значительно уступают возможностям вышеупомянутых субъектов, осуществляющих обработку данных. При этом административное право демонстрирует уникальные преимущества в решении данных проблем.

Прежде всего, следует отметить, что применение публично-правовых мер (информационно-правовых, административных, конституционных) обеспечения безопасности персональных данных граждан по сравнению с гражданским и

---

[376] *Ли Синюй.* Исследование по административно-правовой защите персональных данных в эпоху больших данных. Газета национальностей в Гуйчжоу.18 марта 2025 г. Выпуск B02.

уголовным правом обладает значительными преимуществами. На самом деле, защита персональной информации от несанкционированного доступа представляет собой комплексную правовую категорию, охватывающую множество механизмов, закрепленных в различных отраслях права. Среди этих нормативных правовых актов, направленных на обеспечение безопасности персональных данных, гражданское и уголовное право в основном сосредоточены на реагировании после совершения противоправных действий, что обуславливает наличие определённых ограничений.

В свою очередь, система публично-правового обеспечения безопасности персональных данных обеспечивает более детальную и систематическую защиту, сочетая как предварительные, так и последующие меры. И как указывалось нами ранее, особенностью обеспечения безопасности персональных данных является то, что меры защиты практически всегда могут быть рассмотрены в системе мер, направленных на обеспечение безопасности персональных данных. Это позволяет эффективно предупреждать нарушения прав граждан путем регулирования деятельности операторов персональных данных, в том числе публичных, и осуществления надзора за их действиями.

Кроме того, органы исполнительной власти обладают уникальными организационными и управленческими преимуществами, что делает их авторитетными, технологически оснащенными и эффективными участниками административной системы. Благодаря этому они способствуют разрешению конфликтов между частными структурами и балансированию интересов сторон, тем самым защищая законные права и интересы граждан.[377] В этой связи публично-правовые меры является весьма эффективными и играют ключевую роль в защите прав и интересов граждан в сфере персональных данных от незаконных посягательств.

2) Органы исполнительной власти постепенно становятся одним из ключевых субъектов, нарушающих права на персональные данные. Обладая значительными возможностями для сбора информации, государственные

[377] *Чжан Хэ.* Исследование системы защиты прав на личную информацию // Финанс эпохи. 2018. № 26. С. 24-25.

структуры могут аккумулировать обширные массивы персональных данных в процессе выполнения своих функциональных обязанностей. Интеграция и использование этих данных способствуют, с одной стороны, повышению эффективности управления административными образованиями на государственном уровне; однако, с другой стороны, существует риск неправомерной обработки персональных данных вследствие злоупотребления властью со стороны уполномоченных органов.

Например, персональные данные могут обрабатываться без предварительного получения согласия субъекта персональных данных [378], в отдельных местных органах власти при осуществлении правительственного раскрытия информации происходит непосредственная публикация конфиденциальных личных данных, таких как имена, номера удостоверений личности и адреса проживания граждан из социально уязвимых групп населения без предварительной анонимизации. Данная практика приводит к нарушению конфиденциальности персональных данных, подрывает доверие граждан к государственным институтам и может быть расценена как ущемление прав субъектов персональных данных.[379]

Так, субъекты административного управления могут выступать в качестве нарушителей прав граждан в сфере защиты персональных данных [380]. Следовательно, обработка персональных данных указанными субъектами требует более детальной законодательной регламентации. Вместе с тем существующие гражданско-правовые и уголовно-правовые средства не в полной мере обеспечивают контроль за деятельностью административных органов и их должностных лиц. Это обусловливает необходимость дальнейшего развития административно-правового регулирования как специального механизма обеспечения безопасности персональных данных.

---

[378] *Минбалеев А. В.* Проблемы обработки персональных данных журналистами и СМИ // Вестник УрФО. Безопасность в информационной сфере № 2(4). 2012. С. 26.

[379] См.: *Цуй Мэнсюэ.* Исследование административно-правовой системы защиты личной информации // Шанхайское правовое исследование. 2020. № 19. С. 37-46.

[380] *Ван Гуанлун.* Административно-правовые меры по обеспечению безопасности персональных данных при раскрытии информации правительством в Китае // Вестник Санкт-Петербургского университета. Право. 2024. № 3. С. 815-834.

Усложнение современной социально-экономической сферы приводит к тому, что общественные отношения становятся более дифференцированными и профессионализированными. Это объективно усиливает роль государства в управлении публичными делами и обусловливает расширение административных полномочий во многих правопорядках. Вместе с тем расширение публичной власти требует надлежащих правовых ограничений, поскольку в противном случае возрастает риск её неправомерного использования. Поэтому отсутствие эффективного публично-правового механизма обеспечения безопасности персональных данных может создавать угрозу нарушения прав граждан со стороны органов публичной власти.

Таким образом, только при наличии системного механизма обеспечения безопасности персональных данных субъекты административного управления могут реализовывать свои полномочия в установленных законом пределах. Такой механизм препятствует злоупотреблению публичной властью и снижает риск нарушения прав и законных интересов граждан в отношении их личной информации. В этом смысле обеспечение безопасности персональных данных выступает необходимым условием законной административной деятельности и построения общества, основанного на принципе верховенства права.

## 2. Развитие публично-правового обеспечения безопасности персональных данных в условиях развития современных цифровых технологий

Полагаем, что совершенствование системы публично-правового обеспечения безопасности персональных данных в условиях развития современных цифровых технологий требует обращения к ряду теоретических концепций, раскрывающих правовую природу персональных данных и особенности их защиты. Рассмотрение этих концепций позволяет определить их значение для построения более последовательного механизма обеспечения безопасности персональных данных.

**1) Теория информационного самоопределения.** Право на самостоятельное определение использования информации предполагает, что гражданин вправе самостоятельно решать, может ли его личная информация собираться,

использоваться или передаваться третьим лицам. Сущность данного права заключается в возможности контролировать условия сбора, обработки и передачи личных данных другим субъектам. В рамках этой теории личная информация рассматривается в тесной связи с достоинством гражданина. Если государственные учреждения, юридические лица или другие граждане собирают личные данные без согласия их владельца, то это ставит субъект информации в положение, где его права нарушаются, а баланс контроля над данными утрачивается. Право на самоопределение занимает центральное место в рассматриваемой теории. Согласно этому подходу, гражданин самостоятельно определяет значение принадлежащей ему информации и решает, давать ли согласие на её сбор и использование. Обработка персональных данных государственными органами или иными субъектами без добровольного волеизъявления лица рассматривается как вмешательство в сферу информационного самоопределения и как возможное ущемление его личных интересов. При этом правовая защита информации не ставится в зависимость от её предварительной классификации: ключевым критерием выступает право гражданина самому решать вопрос о предоставлении своих персональных данных. Это теория охватывает весь спектр информации, связанной с гражданином, независимо от её значимости – будь то ценная или не имеющая практической пользы информация.

В условиях стремительного развития современных цифровых технологий (больших данных, искусственного интеллекта, технологий виртуальной реальности и др.) государственные и муниципальные органы и другие операторы вынуждены собирать или обрабатывать значительные объемы персональных данных граждан в соответствии с потребностями публичного управления, необходимостью предоставления государственных услуг, а также других нужд. Хотя граждане могут получить множество преимуществ от этих процессов, существует риск неконтролируемого сбора или обработки персональных данных как со стороны государственных, так и частных операторов, что может привести к серьёзным негативным последствиям для защиты права на персональные

данные.[381]

Как мы уже подчеркивали ранее, взаимосвязь между защитой персональных данных и их сбором или обработкой операторами следует всегда рассматривать с диалектической точки зрения. С одной стороны, для обеспечения рациональности и эффективности предоставляемых услуг и осуществления бизнес-деятельности операторам необходимо получать значительный объем персональных данных для анализа и обработки, что используется для достижения более точного и научно обоснованного административного планирования, а также для производственных и эксплуатационных целей. В то же время на практике операторам, прежде всего государственным органам, не всегда удаётся установить достаточно определённые стандарты и границы сбора и обработки данных. Подобная неопределённость может способствовать возникновению утечек личной информации и иных нарушений в сфере обращения с персональными данными. Дополнительную проблему создаёт то, что некоторые операторы не обеспечивают надлежащий уровень защиты крупных массивов собранной информации, вследствие чего возрастает риск нарушения прав и законных интересов граждан. В связи с этим теория права на информационное самоопределение имеет значение для обоснования пределов деятельности операторов и формирования правовой основы защиты информационных прав личности.

**2) Теория принципа пропорциональности.** Принцип пропорциональности является одним из основных начал современного публичного права и предполагает соразмерность между целями административной деятельности и средствами их достижения. Органы публичной власти при принятии решений должны учитывать права и законные интересы лиц, затрагиваемых соответствующими мерами, а также оценивать возможные последствия вмешательства в частную сферу. Особое значение имеет проверка того, может ли публичная цель быть достигнута менее обременительными средствами. В контексте защиты личной информации это означает необходимость разумного

[381] *Ли Цзяньсинь.* Защита личной информации и раскрытие административной информации в четырех местах по обе стороны пролива // Юридическая наука. 2013. № 7. С. 26-27.

соотношения между административной целью сбора или раскрытия персональных данных и возможным ущербом для граждан.

В структуре принципа пропорциональности обычно выделяются три основных элемента:

а) Принцип целесообразности, согласно которому административные действия должны преследовать законную и публично значимую цель. Это означает, что органы государственной власти и их сотрудники могут раскрывать, собирать и использовать личную информацию граждан исключительно для достижения общественных интересов и выполнения функций административного управления. Указанный принцип предполагает, что раскрытие личной информации должно осуществляться только по обоснованным и законным основаниям. Целью раскрытия является обеспечение права общества на информацию и формирование прозрачного и справедливого государства, а не достижение неправомерных или недобросовестных целей. Более того, раскрытие личной информации граждан должно способствовать реализации социальных и общественных задач. При раскрытии личной информации органы государственной власти обязаны определять способы, формы и временные рамки такого раскрытия с учётом публичного интереса, принципа соразмерности и необходимости недопущения избыточного ограничения прав граждан.[382]

б) Принцип необходимости предполагает, что органы публичной власти вправе раскрывать личную информацию граждан только при наличии объективной потребности и при отсутствии иных средств достижения публично значимой цели. При этом объём и способ раскрытия должны быть ограничены пределами, действительно необходимыми для решения соответствующей задачи. Такой подход позволяет обеспечить баланс между публичным интересом и защитой частной жизни, а также предотвращает необоснованное вмешательство в сферу прав и законных интересов граждан.

в) Принцип пропорциональности в узком смысле, который подразумевает

---

[382] *Ли Вэй.* Переосмысление и реконструкция иерархической теории принципа пропорциональности // Вестник Ичуньского колледжа. 2020. № 4. С. 37-40.

анализ соотношения затрат и выгод от административных действий соответствующих органов. Выгоды, получаемые органами власти в результате использования и совершения иных действий с персональными данными граждан, должны значительно превышать связанные с этим расходы. Органы публичной власти обязаны оценивать баланс между частными интересами граждан (включая возможный ущерб, причиненный раскрытием личных данных), а также социальными и общественными интересами, которые сохраняются после раскрытия информации. При такой оценке необходимо учитывать два основных критерия: степень конфиденциальности персональных данных граждан и значимость публичного интереса. В случаях, когда публичный интерес, защищаемый органами власти, имеет преобладающее значение, раскрытие данных может быть признано допустимым. Напротив, если соответствующие сведения обладают высокой степенью конфиденциальности, приоритет должен отдаваться их сохранению в закрытом режиме.[383]

3) Теория административной помощи исходит из того, что наличие у гражданина субъективного права предполагает возможность его реальной защиты. В случае нарушения прав противоправными действиями третьих лиц должны быть обеспечены надлежащие механизмы восстановления нарушенного положения. Данный подход применим и к сфере персональных данных. Если органы государственной власти или иные организации с нарушением закона собирают, раскрывают либо используют персональные данные, создавая риск причинения вреда правам и законным интересам субъектов данных, последние должны иметь возможность восстановить нарушенные права с помощью законных и обоснованных средств защиты.

По сравнению с иными средствами правовой защиты административная помощь, как правило, предполагает участие органов публичной власти. При этом отношения между такими органами и гражданами изначально не являются равными, поскольку публичная власть обладает властными полномочиями. В

[383] *Дай Синь, Чжан Юнцзянь.* Принцип пропорциональности или критическая реконструкция правовых методов анализа затрат и выгод // Китайское и иностранное право. 2018. № 6. С. 1519-1545.

связи с этим при оказании административной помощи необходимо соблюдать ряд специальных принципов[384]:

Прежде всего, при оказании административной помощи органы публичной власти и их должностные лица должны действовать объективно и независимо, обеспечивая защиту прав и законных интересов субъектов персональных данных. Ко всем участникам процесса следует относиться одинаково, беспристрастно и объективнее, не только с точки зрения материальных прав, но и защищать законные права и интересы участников с точки зрения процедур.[385] В настоящее время существует риск нарушения нейтральности со стороны органов пересмотра из-за тесных связей с ответчиком, что может повлиять на справедливость процесса.

Во-вторых, запрещены неблагоприятные изменения. В случае несогласия гражданина с применением законодательства о защите персональных данных, а также с действиями или решениями органа публичной власти и его должностных лиц, он вправе воспользоваться предусмотренными законом средствами защиты. При пересмотре такого дела должно соблюдаться правило недопустимости ухудшения положения заявителя по сравнению с первоначальным административным актом.

В частности, если по результатам рассмотрения жалобы орган административного пересмотра признаёт первоначальное административное решение соответствующим требованиям закона, такое решение может быть оставлено в силе. Вместе с тем недостаточная строгость применённой меры ответственности сама по себе не даёт органу пересмотра права усиливать санкцию, если это приводит к ухудшению положения заявителя. В такой ситуации его полномочия должны сводиться к отмене незаконного решения либо к применению иных процессуально допустимых мер.

Значение данного принципа заключается в том, что он гарантирует субъекту персональных данных возможность обращаться за правовой защитой без риска

---

[384] *Ван Цзинбинь, Чжан Цинъянь.* О принципах предоставления административной помощи в Китае // Журнал Северо-Восточного педагогического университета. Философские и общественные науки. 2008. № 2. С. 50-55.

[385] *Чжоу Юйон.* Исследование основных принципов административного права. Ухань: Издательство Уханского университета. 2005. С. 250.

ухудшения своего положения.[386] Ухудшение положения заявителя вследствие обращения за правовой защитой противоречит самой природе данного института и снижает эффективность защиты прав и законных интересов субъекта персональных данных.

Наконец, необходимо учитывать принцип своевременности оказания помощи. Органы публичной власти обязаны рассматривать споры в сфере защиты персональных данных без необоснованных задержек, одновременно соблюдая установленные процедурные требования и принцип процессуальной справедливости. Несвоевременное реагирование на нарушение прав в отношении личной информации способно расширить масштаб вредных последствий и затруднить восстановление нарушенного положения субъекта персональных данных.

### 3. Недостатки публично-правового обеспечения безопасности персональных данных в Китае и России

Законодательство многих государств, включая Россию и Китай, содержит положения, обеспечивающие безопасность персональных данных. Однако многие проблемы остаются нерешенными[387], что требует дальнейшего совершенствования правового регулирования сбора и обработки персональных данных, обеспечения их безопасности путем предоставления эффективных правовых режимов для разных персональных данных и разработки современной модели контроля информационной безопасности.

Вышеизложенный анализ демонстрирует, что недостатки публично-правового обеспечения безопасности персональных данных в Китае и в России проявляются, главным образом, в следующем.

1) Существенные различия в правовых основаниях наложения административных санкций за нарушения, связанные с обработкой персональных данных граждан. Поскольку административная ответственность за нарушение законодательства о персональных данных в России единообразно предусмотрена в

---

[386] *Цай Чжифан.* Новая теория права административной помощи. Пекин: Издательство Юань-Чжао. 2001. С. 96.
[387] *Чернусь, Н. Ю., Чжун, Я.* Проблемы правовой защиты персональных данных по законодательству России и Китая. Respublica Literaria. Т. 5. № 1. 2024. С.113-123.

КоАП РФ, нет никаких проблем в том, что правовая основа для применения административных наказаний неодинакова. Однако применение административных наказаний в Китае за персональные данные предусмотрено в разных законах[388], поэтому возникли проблемы, связанные с несогласованностью правовых оснований по применению административных наказаний.

2) Недостатки в системе административного контроля, касающегося обеспечения защиты персональных данных. По мере принятия ряда законов и подзаконных актов, таких как Закон КНР о ПДн, ФЗ о ПДн и ряд других нормативных правовых актов, правовая база для защиты личной информации в Китае в России в основном была уже сформирована[389]. Однако в Китае и России по-прежнему наблюдаются различные виды нарушений в области персональных данных[390], при этом эффективность надзорных мер остается на недостаточно высоком уровне. Данная ситуация в Китае проявляется, главным образом, в двух аспектах: а) отсутствие четкого распределения обязанностей между различными департаментами в процессе осуществления контроля; б) низкая результативность работы органов, ответственных за надзор в данной сфере. В России основная проблема связана с высоким уровнем утечек персональных данных.

3) Несовершенство системы административной помощи по защите персональных данных. В Китае в случае нарушения органами исполнительной власти конфиденциальности личной информации граждане, как правило, могут воспользоваться механизмом административного пересмотра либо обратиться в суд с административным иском. Несмотря на то что указанные средства способны

---

[388] Например, в статье 64 Закона КНР о кибербезопасности, статья 66 Законе КНР о ПДн, статье 45 Закона КНР о безопасности данных, статье 56 Закона КНР о защите прав и интересов потребителей содержится административная ответственность.

[389] *Ван Гуанлун.* Механизм административно-правового регулирования защиты персональных данных в Китае: состояние, недостатки и путь решения // Вестник Московского университета. 2024. Серия 11. Право. Том 65. № 4. С. 204-232.

[390] Например, по данным исследования Центра цифровой экспертизы Роскачества, опубликованного в 2024 году, 76,7% приложений для заказа такси имеют проблемы с защитой персональных данных; по данным исследования Центра цифровой экспертизы Роскачества, опубликованного в 2024 году, 76,7% приложений для заказа такси имеют проблемы с защитой персональных данных; по данным ежегодного исследования «СёрчИнформ», посвящённого уровню информационной безопасности в России, в 2024 году организации чаще всего сталкивались со сливами информации о клиентах и сделках (44%) и персональных данных (36%). URL: https://habr.com/ru/news/849334/; https://www.comnews.ru/content/231651/2024-02-20/2024-w08/1008/rossiyskie-sayty-zabyli-pro-politiki-konfidencialnosti; https://rg.ru/2025/02/26/messendzhery-na-pricele.html?ysclid=maak9gkpj554031984 (дата обращения: 05.05.2025).

обеспечивать защиту прав в сфере персональных данных, их практическое значение зависит от эффективности соответствующих процедур. Если административные механизмы защиты остаются недостаточно развитыми или применяются формально, обеспечение надлежащей охраны личной информации существенно осложняется.

4) Недостатки в защите личной информации в процессе открытия государственных данных. Реализуемые в Китае и России меры по обеспечению открытости государственных данных позволяют сделать процедуры запроса и получения информации более прозрачными и менее обременительными для заявителей. Однако необходимо подчеркнуть, что система открытия государственных данных в обоих государствах все еще находится на этапе развития, а также наблюдаются значительные пробелы в защите персональных данных при раскрытии информации. Так, существующие проблемы в основном отражены в трех аспектах: а) низкий уровень законодательства, регулирующего открытое использование и доступ к данным; б) противоречие между раскрытием правительственной информации и защитой личной информации с точки зрения защиты законных интересов, и в) чрезмерная власть правительства над сбором и раскрытием персональных данных[391].

**4. Рекомендации по решению актуальных проблем в сфере публично-правового обеспечения безопасности персональных данных в Китае и России**

С развитием науки и техники происходит трансформация структуры социальных интересов, а также эволюция национальной публичной модели управления в сфере персональных данных. Информационные, в том числе цифровые, технологии вызвали комплексные изменения во всех сферах общества, способствуя как модернизации технического уровня развития, так и созданию новых вызовов в области защиты персональных данных. С одной стороны, стремительное развитие информационных технологий существенно расширило возможности государственных органов по обработке данных, сократило

[391] *Ван Гуанлун.* Механизм административно-правового регулирования защиты персональных данных в Китае: состояние, недостатки и путь решения // Вестник Московского университета. 2024. Серия 11. Право. Том 65. № 4. С. 204-232.

административные издержки современного общества и повысило качество предоставляемых государственных услуг. С другой стороны, по мере возрастания ценности информации, возникает необходимость в постоянном сборе и ее использовании. Благодаря внедрению инновационных технологий персональные данные граждан могут распространяться и публиковаться в сети Интернет в любое время и в любом месте, что привлекает повышенное внимание к вопросам их защиты. В связи с этим защита личной информации исключительно на основе традиционного правового регулирования оказывается недостаточной. Необходимо стимулировать государственные органы к совершенствованию системы защиты персональных данных через усиление публично-правовых механизмов обеспечения их безопасности.

1) Уточнение иерархической взаимосвязи между различными нормативными правовыми актами в процессе их применения в Китае представляет собой важную задачу. В практике административных наказаний за защиту персональных данных необходимо обеспечить надлежащее регулирование выборочного применения правовых норм, содержащих в ряде законов[392]. Анализ мнения ряда ученых позволил выделить следующие аспекты[393].

а) Административные санкции, закреплённые в законах и подзаконных актах о защите личной информации, в общем порядке должны применяться с учётом положений Закона КНР об административных наказаниях и Закона КНР о наказаниях за нарушение общественного порядка. Эти положения имеют значение как для определения содержания мер ответственности, так и для процедуры их установления и применения. Вместе с тем специальные законы или подзаконные акты могут предусматривать особые правила относительно предмета, вида и порядка назначения административных наказаний. В этом случае применяется специальное регулирование, а общие нормы сохраняют значение постольку,

---

[392] Здесь касается таких законов, как Закон КНР о защите персональной информации, Закон КНР об административных наказаниях, Закон КНР о наказаниях за нарушение общественного порядка, Закон КНР о защите прав потребителей, Закон КНР о кибербезопасности и Закон КНР о безопасности данных.

[393] *Ван Гуанлун.* Механизм административно-правового регулирования защиты персональных данных в Китае: состояние, недостатки и путь решения. // Вестник Московского университета. 2024. Серия 11. Право. Том 65. № 4. С. 204-232.

поскольку они не противоречат таким специальным положениям.[394].

б) Для правильного определения подлежащих применению норм следует учитывать цель соответствующего законодательного акт[395]а, характер нарушенных законных интересов, основания привлечения к административной ответственности, а также функциональное назначение конкретного правового требования. Так, нормы Закона КНР о защите прав потребителей защищают права и законные интересы потребителей в отношении их личной информации, однако их применение обусловлено наличием отношений потребительского характера. Закон КНР о безопасности данных имеет иную направленность: он связан прежде всего с обеспечением безопасности данных, защитой национального суверенитета, государственной безопасности и интересов развития. В нём отдельно акцентируются вопросы общедоступных данных и трансграничной безопасности данных, что отличает сферу его применения от сферы действия Закона КНР о персональных данных.

в) В условиях конкуренции норм, устанавливающих ответственность за нарушения в сфере персональных данных, необходимо согласовывать формулировки положений об ответственности в различных правовых актах. Это позволит снизить риск произвольного применения таких норм уполномоченными органами и ограничить влияние ведомственных интересов на выбор меры ответственности.

2) Интеграция ресурсов сетевого надзора и усиление механизмов контроля с применением технологий больших данных представляют собой ключевые направления в современной цифровой эре. Защита личной информации имеет важное значение для множества заинтересованных сторон. Необходимо не только максимально эффективно использовать потенциал персональных данных, но и обеспечивать полную защиту законных прав и интересов соответствующих субъектов. В условиях надзора за безопасностью персональных данных

---

[394] *Ван Гуанлун.* Механизм административно-правового регулирования защиты персональных данных в Китае: состояние, недостатки и путь решения. // Вестник Московского университета. 2024. Серия 11. Право. Том 65. № 4. С. 204-232.

[395] То есть, такие законы как Закон КНР о защите персональной информации, Закон о защите прав потребителей, Закон о кибербезопасности и Закон о безопасности данных.

традиционная зависимость от единого органа исполнительной власти уже не удовлетворяет потребностям более активного внедрения цифровых технологий, в том числе больших данных. Таким образом, интеграция сил по контролю за сетью Интернет становится неотъемлемой частью повышения эффективности административного надзора, что включает в себя два основных аспекта:

а) Необходимо поэтапно создавать совершенную интегрированную платформу для мониторинга персональных данных, обеспечивающую поддержку регулирующим органам за счет объединения информации из различных источников. Это включает как расширение каналов сбора данных, так и предоставление гражданам возможности оперативной обратной связи по вопросам, связанным с мониторингом личной информации, что позволит максимально активизировать роль общественного контроля.

б) Механизм координационного надзора должен постепенно совершенствоваться, при этом органы исполнительной власти, независимые третьи стороны и иные участники после выполнения своих функций по надзору могут обмениваться полученными данными. Такой подход обеспечивает передачу информации между регулирующими органами, способствуя формированию единой системы взаимодействия и повышению эффективности межведомственной координации.[396]

3) Совершенствование системы административной помощи в сфере защиты персональных данных и усиление развития административного судопроизводства в интересах общественности приобретают особую актуальность. Применение больших данных и иных цифровых технологий придаёт нарушениям прав на персональную информацию ряд специфических черт[397]:

Во-первых, технологизация процесса. С одной стороны, развитие сетевых технологий облегчило доступ к цифровым сервисам и повысило удобство их использования. С другой стороны, оно одновременно обострило проблему

---

[396] *Ли Япин, Чжоу Вэйлян.* Стратегия динамического надзора за защитой личной информации в режиме онлайн // Журнал Чунцинского технологического университета. Общественные науки. 2021. № 11. С. 25-134.

[397] *Ван Гуанлун.* Механизм административно-правового регулирования защиты персональных данных в Китае: состояние, недостатки и путь решения // Вестник Московского университета. 2024. Серия 11. Право. Том 65. № 4. С. 204-232.

защищённости персональных данных. Современные технологии, включая отслеживание файлов cookie и мониторинг сетевой активности, создают условия для скрытого сбора и дальнейшего использования информации. Это, в свою очередь, затрудняет выявление соответствующих нарушений и своевременное реагирование на них.[398]

Во-вторых, данный аспект проявляется в латентном характере нарушений информационных прав и утрате их чёткой территориальной привязки. Проведённый анализ показывает, что как участники рынка, так и органы исполнительной власти всё чаще осуществляют свою деятельность через интернет-платформы. В этих условиях субъектам информационных прав становится значительно сложнее выявить факт нарушения, доказать время и место его совершения, а также установить ответственных лиц. Трансграничная природа интернета дополнительно способствует продаже и распространению личной информации за пределами национальной юрисдикции, что повышает устойчивость и повторяемость подобных нарушений.

В-третьих, последствия нарушений в сфере персональных данных отличаются высокой степенью общественной и правовой значимости. Инциденты, связанные с утечкой такой информации, затрагивают различные аспекты правового положения личности и могут привести к существенному ущербу для прав, законных интересов и безопасности граждан. Персональные данные не только представляют экономическую ценность для их владельцев, но и имеют специфическое значение в контексте защиты частной жизни [399] . После компрометации персональной информации восстановление прежнего уровня её защищённости становится крайне сложным. Дело Сюй Юйюй показывает, что утечка личной информации способна привести не только к имущественному или репутационному ущербу, но и к наиболее тяжёлым последствиям для жизни и

[398] *Юань Дуньлян.* Уголовно-правовая защита личной информации при использовании технологии cookie // Журнал западных исследований. 2021. № 22. С. 56-58.
[399] *Ван Гуанлун.* Механизм административно-правового регулирования защиты персональных данных в Китае: состояние, недостатки и путь решения // Вестник Московского университета. 2024. Серия 11. Право. Том 65. № 4. С. 204-232.

безопасности человека.[400]

Учитывая вышеуказанные характеристики нарушений прав на персональные данные, автор считает целесообразным предоставить гражданам свободу самостоятельного выбора. То есть, в случае нарушения личной информации гражданина уполномоченным органом, решение о подаче ходатайства об административном пересмотре или (и) инициировании административного иска должно полностью находиться в компетенции самого субъекта информации. Помимо этого, необходимо усилить развитие административного судопроизводства для защиты интересов общественности[401].

Суть системы судопроизводства в интересах общественности заключается в защите публичных интересов общества, что предполагает наличие у предмета данного типа судопроизводства публичных атрибутов. В условиях развития больших данных личная информация не может быть полностью отнесена к частным правам отдельных граждан. С одной стороны, государство собирает и обрабатывает значительные объемы персональных данных граждан в процессе осуществления публичного управления, при этом данные перестают быть исключительно частной собственностью лиц и становятся важным инструментом для выполнения государственных функций органами исполнительной власти. С другой стороны, использование алгоритмических технологий для интеграции и анализа данных оказывает существенное влияние на общество и общественные интересы. Таким образом, личная информация граждан приобрела публичные характеристики, что обосновывает включение дел по защите персональных

---

[400] В 16:30 19 августа 2016 года Сюй Юйюй, которая только что поступила в Нанкинский университет почты и телекоммуникаций, получила странный звонок. Собеседник сказал, что он из Бюро образования и ей должен быть присужден грант (на самом деле этот звонок был от телекоммуникационный мошенник). Впоследствии Сюй Юйюй последовала инструкциям «активировать учетную запись» и перевела 9 900 юаней, которые должны были пойти на оплату обучения, на счет, предоставленный мошенником. Днем 19 августа, обнаружив, что ее обманули, Сюй Юйюй была очень опечалена. Той ночью, по дороге домой Сюй Юйюй внезапно упала в обморок и была без сознания, а позже умерла после безуспешной попытки спасения. В данном случае утечка личной информации Сюй Юйюй была основной причиной его смерти от мошенничества. См.: Прокурор объяснил процесс рассмотрения дела о смерти Сюй Юйюй в результате телекоммуникационного мошенничества: URL: https://www.spp.gov.cn/zdgz/201706/t20170627_194085.shtml (дата обращения: 14.01.2024).

[401] *Ван Гуанлун.* Механизм административно-правового регулирования защиты персональных данных в Китае: состояние, недостатки и путь решения // Вестник Московского университета. 2024. Серия 11. Право. Том 65. № 4. С. 204-232.

данных в категорию судебного производства в общественных интересах[402].

В соответствии со статьей 70 Закона КНР о ПДн, право подачи административного иска в интересах общественности предоставлено органам прокуратуры, организациям потребителей и организациям, аккредитованным Государственной администрацией по делам киберпространства. Это свидетельствует о том, что на законодательном уровне в Китае уже установлена система судебного разбирательства в защиту общественных интересов в сфере защиты персональных данных.

Вместе с тем, сложность для граждан самостоятельного отстаивания своих прав при нарушении личных данных также стала предметом широкого общественного внимания. Значение статьи 70 заключается в расширении круга субъектов, уполномоченных инициировать административные дела в защиту общественных интересов. Наряду с органами прокуратуры такое право предоставлено организациям по защите прав потребителей и организациям, аккредитованным Государственной администрацией по делам киберпространства. Данный подход учитывает особенности нарушений в сфере личной информации и специфику публично-правовой защиты общественных интересов, создавая основу для дальнейшего развития этого института. Вместе с тем следует учитывать и существующие недостатки данного регулирования. Формулировка «организации, определённые Государственной администрацией по делам киберпространства» остаётся недостаточно определённой и требует дальнейшего уточнения. В перспективе это может потребовать принятия специальных разъяснений или судебных толкований, направленных на конкретизацию критериев отнесения организаций к данной категории.[403]

В руководящих примерах, опубликованных Верховной народной прокуратурой 7 марта 2022 года, в рамках дела о надзоре Пекинской муниципальной прокуратуры за административными судебными

[402] *Ван Гуанлун.* Механизм административно-правового регулирования защиты персональных данных в Китае: состояние, недостатки и путь решения // Вестник Московского университета. 2024. Серия 11. Право. Том 65. № 4. С. 204-232.

[403] *Ван Гуанлун.* Механизм административно-правового регулирования защиты персональных данных в Китае: состояние, недостатки и путь решения // Вестник Московского университета. 2024. Серия 11. Право. Том 65. № 4. С. 204-232.

разбирательствами в интересах общественности по защите личной информации детей, Верховная народная прокуратура чётко подтвердила, что при наличии нарушений персональных данных несовершеннолетних вследствие недостаточного контроля со стороны уполномоченных органов исполнительной власти, органы прокуратуры имеют право инициировать административные иски в защиту общественных интересов.[404] Следовательно, становится очевидным[405], что в процессе анализа судебной практики по конкретным делам органы прокуратуры постепенно включают вопросы защиты личной информации граждан, особенно несовершеннолетних, в сферу рассмотрения дел в интересах общественности[406].

Таким образом, в условиях цифровой трансформации важность персональных данных и обеспечения их безопасности становится очевидной. Органы исполнительной власти осуществляют обработку персональных данных граждан для обеспечения более эффективного и научно обоснованного выполнения административных функций, направленных на общественное благосостояние. В свою очередь, субъекты рынка используют персональные данные для оптимизации затрат и достижения значительных экономических выгод. Однако нельзя упускать из виду, что в последние годы как органы исполнительной власти, ориентированные на общественные интересы, так и коммерческие организации, преследующие частные цели, периодически нарушают права и законные интересы субъектов персональных данных. В результате обеспечение безопасности личной информации стало актуальной проблемой, требующей внимания разных государств мира[407].

4) Непрерывное развитие и совершенствование механизма раскрытия государственных данных требует системного подхода. Безусловно, открытая

---

[404] См.: 35-я группа руководящих дел Верховной Народной прокуратуры, опубликованная 07 марта 2022 года: URL: https://www.spp.gov.cn/spp/xwfbh/wsfbh/202203/t20220307_547722.shtml (дата обращения: 14.01.2024).

[405] *Ван Гуанлун.* Механизм административно-правового регулирования защиты персональных данных в Китае: состояние, недостатки и путь решения. // Вестник Московского университета. 2024. Серия 11. Право. Том 65. № 4. С. 204-232.

[406] *Ван Гуанлун.* Механизм административно-правового регулирования защиты персональных данных в Китае: состояние, недостатки и путь решения. // Вестник Московского университета. 2024. Серия 11. Право. Том 65. № 4. С. 204-232.

[407] *Ван Гуанлун.* Механизм административного-правового регулирования защиты персональных данных в Китае: состояние, недостатки и путь решения. // Вестник Московского университета. 2024. Серия 11. Право. Том 65. № 4. С. 204-232.

эксплуатация государственных данных представляет собой инновационную конструкцию системы управления, которая также является значительной реформой для проверки эффективности управления различными государственными учреждениями. В процессе практической реализации она сталкивается с множеством препятствий, поэтому необходимо постоянно совершенствовать данный механизм как на теоретическом уровне, так и в практическом применении. В частности важно:

Во-первых, на основе принципа пропорциональности сбалансировать противоречивые отношения между общественными интересами и законными личными интересами. С позиции органов государственной власти можно отметить, что в большинстве случаев защита персональных данных граждан и раскрытие государственных данных представляют собой два аспекта одной проблемы.[408] Другими словами, раскрытие государственных данных и защита персональных данных формируют антагонистические отношения, отражающие баланс между общественными и индивидуальными интересами. Таким образом, раскрытие государственной информации должно оцениваться с позиции его соразмерности защите конфиденциальности личных данных. Такой подход позволяет согласовать публичный интерес в доступе к информации с необходимостью охраны персональных данных. Регулирование коллизий между этими интересами может осуществляться с учётом двух основных аспектов[409]:

а) Прежде всего требуется уточнить содержание ключевых понятий. В процессе раскрытия правительственной информации необходимо проводить чёткое различие между личной и конфиденциальной информацией, что позволяет обеспечить более последовательную защиту персональных данных граждан.[410] С юридической точки зрения личная информация представляет собой особый объект правовой охраны, обладающий комплексной природой и включающий, наряду с

---

[408] *Чжоу Ханьхуа.* Закон Китайской Народной Республики о защите персональной информации (проект рекомендаций экспертов) и отчет об исследовании законодательства. Пекин: Юридическая пресса. 2006. С. 64.

[409] *Ван Гуанлун.* Административно-правовые меры по обеспечению безопасности персональных данных при раскрытии информации правительством в Китае. // Вестник Санкт-Петербургского университета. Право. 2024. № 3. С. 815-834.

[410] *Кун Фаньхуа.* Защита личной конфиденциальности при раскрытии правительственной информации // Исследование административного права. 2020. № 1. С. 17-29.

личными неимущественными характеристиками, определённые имущественные элементы. Конфиденциальность, в отличие от персональной информации, ориентирована прежде всего на охрану частной сферы и сведений, не предназначенных для раскрытия. Механизм возмещения вреда обычно применяется уже после незаконного разглашения таких сведений. С точки зрения объекта защиты конфиденциальность связана главным образом с неприкосновенностью частной жизни и сохранением её тайны, тогда как персональная информация включает более широкий массив данных, относящихся к личности человека и его идентификации. В связи с этим разграничение личной и конфиденциальной информации необходимо для того, чтобы государственные органы осуществляли раскрытие информации правомерно и с учётом допустимых пределов вмешательства в частную сферу.[411]

б) Раскрытие правительственной информации должно осуществляться с учётом публичного интереса, но это не освобождает государство от обязанности защищать персональную информацию граждан. При столкновении общественного интереса с правами отдельных лиц приоритет публичного интереса допустим лишь при наличии достаточных правовых оснований и соблюдении принципа пропорциональности. Если же сведения, относящиеся к частной жизни, не имеют прямой связи с общественно значимой целью, право на конфиденциальность должно сохранять приоритетную защиту. Поэтому при раскрытии государственных данных необходимо разумно разграничивать сферу публичных и частных интересов, используя принцип пропорциональности как инструмент оценки допустимого вмешательства. В этих условиях целесообразно внедрить механизм оценки рисков, позволяющий определить, насколько раскрытие правительственной информации является обоснованным, необходимым и соразмерным. Такая оценка должна учитывать как задачи общественной безопасности и публичного управления, так и возможные последствия для прав граждан. Конкретные этапы оценки рисков могут включать следующие элементы:

---

[411] *Ван Гуанлун.* Административно-правовые меры по обеспечению безопасности персональных данных при раскрытии информации правительством в Китае // Вестник Санкт-Петербургского университета. Право. 2024. № 3. С. 815-834.

- Если раскрытие правительственной информации не отвечает критериям целесообразности, это даёт основание говорить о нарушении принципа пропорциональности при осуществлении публичной власти и о недопустимости соответствующих действий. План оценки должен быть юридически обоснованным и соответствовать этическим стандартам. Субъект, осуществляющий оценку, обязан подтвердить необходимость выбранной модели оценки. Наряду с этим принятие решения должно сопровождаться консультациями с заинтересованными сторонами, что обеспечивает большую прозрачность и обоснованность всей процедуры.[412]

- С учётом принципов пропорциональности и целевого назначения должна проводиться сравнительная оценка публичных и частных интересов. В случаях, когда такая оценка выявляет высокий риск нарушения конфиденциальности персональных данных или неприкосновенности частной жизни в результате раскрытия информации государственными органами либо использования технологий мониторинга больших данных, необходимо применять более строгие критерии допустимости вмешательства в сферу личной информации. При низком уровне риска реализация права общества на информацию может быть признана допустимой, если она служит целям общественной безопасности и социальной стабильности. Наряду с этим важно развивать более чёткие стандарты осуществления административных полномочий, позволяющие обеспечить предсказуемую и правомерную обработку персональных данных.

- С учётом результатов оценки воздействия обработки личных данных субъекту может предоставляться различный объём контроля над соответствующей информацией. Например, персональные данные, собираемые государственными органами для оказания публичных услуг, должны использоваться в пределах первоначально заявленной цели и не могут применяться для иных задач без дополнительного согласия субъекта. Передача таких сведений между государственными учреждениями требует соблюдения дополнительных гарантий,

---

[412] *Цзоу Дуншэн.* Раскрытие правительством данных и защита личной конфиденциальности: пример Канады // Административное управление Китая. 2018. № 6. С. 77.

в том числе получения повторного согласия, если такая передача затрагивает права и законные интересы гражданина. Субъект данных также должен быть уведомлён о целях и способах использования своей информации и обладать возможностью требовать исправления недостоверных сведений.

В рамках данной модели оценки рисков судебный контроль выполняет самостоятельную функцию. Он направлен не на блокирование деятельности законодательных и административных органов, а на проверку соразмерности между реализацией публичной власти и защитой индивидуальных прав. В частности, суд должен оценивать значимость общественного интереса, обосновывающего раскрытие правительственной информации, а также устанавливать, не влечёт ли такое раскрытие чрезмерного вмешательства в сферу личных данных граждан. При необходимости суд может потребовать от компетентного административного органа представить обоснование того, что раскрытие информации действительно необходимо для достижения публично значимой цели. Таким образом, применение методик оценки рисков и механизмов судебного контроля позволяет перевести анализ законных интересов из плоскости субъективных оценок в более рациональную и практически применимую модель правового регулирования.

Во-вторых, требуется дальнейшее совершенствование механизмов правовой защиты персональных данных, а также развитие нормативной базы, регулирующей открытое использование государственных данных. Соответствующие нормативные акты имеют двойное значение: с одной стороны, они создают правовые условия для раскрытия государственных данных, а с другой — обеспечивают пределы и гарантии их правомерного использования. Таким образом, совершенствование правового режима открытого использования государственных данных имеет важное значение для упорядоченного раскрытия информации органами исполнительной власти. В более широком смысле оно является одним из необходимых элементов формирования цифрового государства

в условиях развития технологий больших данных.[413]

Данный вопрос можно рассмотреть на примере Китая. Закон КНР о безопасности данных занимает ключевое положение в существующей системе правового регулирования данных и оказывает руководящее воздействие на макроуровне при регулировании деятельности по обработке данных. Таким образом, законодатель имеет возможность уточнить или дополнить нормы, специфически регулирующие использование общедоступных данных в рамках действующего Закона о безопасности данных. Такой подход позволит избежать избыточного нормативного регулирования и одновременно усилить юридическое значение положений, связанных с открытым использованием государственных данных. По мере формирования необходимых правовых и организационных условий следует рассмотреть возможность систематизации действующего «Положения КНР об открытии государственной информации» и соответствующих нормативных актов, принятых на разных уровнях, с последующей разработкой самостоятельного закона об открытии правительственных данных [414]. Его принятие могло бы обеспечить более последовательную защиту прав и законных интересов заинтересованных субъектов в сфере государственных данных[415].

В-третьих, целесообразно сформировать механизм оценки рисков, связанных с государственными данными, поскольку он позволит более последовательно регулировать обработку персональных данных органами исполнительной власти. В условиях динамичного развития и совершенствования информационных технологий, когда органы исполнительной власти всё активнее внедряют алгоритмы и инновационные технологии для обслуживания общества, возрастает вероятность нарушения права на персональные данные граждан. Таким образом, разработка и внедрение комплексного механизма оценки рисков для государственных данных представляется необходимым шагом для минимизации

---

[413] *Ши Яньцзюнь.* Реальная дилемма открытого использования правительственных данных в эпоху больших данных и пути к его правовому обеспечению // Журнал Пекинского университета почты и телекоммуникаций. Общественные науки. 2023. № 6. С. 81-82.

[414] *Ван Гуанлун.* Административно-правовые меры по обеспечению безопасности персональных данных при раскрытии информации правительством в Китае. // Вестник Санкт-Петербургского университета. Право. 2024. № 3. С. 815-834.

[415] *Ма Яньсинь, Ли Чжэ, Юань Цян и др.* Цифровое правительство: перемены и верховенство закона. Пекин: Издательство Китайского университета Жэньминь. 2021. С. 226.

указанных угроз. Его создание необходимо, поскольку:

а) создание комплексного набора механизмов для оценки рисков, связанных с государственными данными, представляет собой важный этап в совершенствовании системы защиты персональных данных на национальном уровне, что, в свою очередь, способствует повышению эффективности функционирования административных органов;

б) механизм оценки рисков, связанных с данными, позволяет научно идентифицировать потенциальные угрозы безопасности личной информации и обеспечивает профессиональное руководство для органов исполнительной власти в процессе обработки данных. Другими словами, данная система оценки рисков выполняет три ключевые функции[416]: во-первых, органы исполнительной власти могут с помощью анализа рисков своевременно внедрять методологии реагирования, что повышает эффективность принятия решений; во-вторых, она способствует надежному контролю за обработкой персональных данных граждан; в-третьих, граждане через получение отчетов об оценке рисков становятся более осведомленными о мерах защиты данных, что способствует укреплению доверия к государственным структурам.[417]

Процесс разработки механизма оценки рисков для государственных данных может быть структурирован по следующим ключевым направлениям[418]:

- субъект обработки информации должен подтвердить необходимость проведения процедуры оценки рисков в соответствии с установленными принципами и критериями;

- отделы защиты персональных данных на всех уровнях органов власти осуществляют конкретные мероприятия по оценке рисков, принимая во внимание предполагаемый уровень угроз и масштаб воздействия. Содержание оценки охватывает источники данных, их характер, методы сбора персональной

---

[416] *Ван Гуанлун.* Механизм административно-правового регулирования защиты персональных данных в Китае: состояние, недостатки и путь решения // Вестник Московского университета. 2024. Серия 11. Право. Том 65. № 4. С. 204-232.

[417] *Се Яовэнь.* Защита личной информации в электронном правительстве: опыт США и рекомендации // Административное управление в Китае. 2019. № 2. С. 140-146.

[418] *У Цянь, Чэнь Яньлин.* Правовая защита персональных данных в сфере электронного правительства // Журнал Юго-Западного нефтяного университета. Общественные науки. 2022. № 1. С. 86-96.

информации и другие связанные аспекты. В случае выявления рисков, превышающих компетенцию органа соответствующего уровня, соответствующие материалы передаются в вышестоящий уполномоченный орган для последующей оценки и принятия обоснованного решения;

- Подразделения, осуществляющие защиту персональных данных на соответствующих уровнях, обязаны готовить развёрнутые отчёты по результатам оценки рисков. В этих отчётах следует фиксировать возможные угрозы нарушения прав граждан в сфере персональных данных и предлагать обоснованные меры по минимизации выявленных рисков;

- Результаты оценки рисков должны приниматься во внимание субъектами обработки информации при согласовании, реализации и дальнейшем сопровождении соответствующих административных проектов.

В-четвёртых, важным направлением является повышение правовой осведомлённости граждан о способах защиты персональных данных и предусмотренных законом гарантиях.[419]. Граждане должны уделять внимание как профилактическим мерам по защите своей информации[420], так и правильным действиям для эффективной защиты своих прав в случае утечки. В связи с этим повышение правовой осведомлённости граждан о механизмах защиты личной информации, закреплённых в законодательстве Китая и России, имеет самостоятельное значение. Речь идёт, в частности, о праве на удаление данных, праве на исправление неточных сведений, модели «уведомление — согласие» и иных правовых гарантиях. При обращении к веб-сайтам и программному обеспечению гражданам необходимо учитывать порядок сбора персональных данных, содержание согласия на их обработку и объём разрешений, предоставляемых приложениям. Кроме того, ограничение публикации реальных личных сведений в социальных сетях и осторожное использование открытых сетей Wi-Fi могут рассматриваться как элементы индивидуального поведения, направленного на снижение риска утечки конфиденциальной информации и

[419] *Цзян, Паньпань.* Теоретическая дилемма и пути защиты личной информации в эпоху больших данных // Современная информатика. 2019. № 8. С. 153-155.
[420] *Ван Гуанлун.* Административно-правовая защита персональной информации в Китае: недостатки и путь решения // Вестник Университета имени О.Е. Кутафина (МГЮА). 2024. № 10. С. 189-197.

защиту персональных данных.

При выявлении нарушения прав и законных интересов граждан в результате раскрытия либо неправомерной обработки персональных данных они могут обратиться за защитой в уполномоченные органы исполнительной власти. Одновременно следует использовать предусмотренные законом механизмы, в том числе право на удаление данных и право на исправление недостоверной информации, поскольку они позволяют ограничить последствия нарушения и пресечь дальнейшее распространение соответствующих сведений. Если такие меры не обеспечивают прекращения нарушения, гражданин вправе прибегнуть к иным средствам правовой защиты, включая подачу жалоб, исковых заявлений и других процессуальных документов[421].

Таким образом, обращение персональных данных и их активное использование в условиях цифровизации становятся значимым фактором экономического развития государства. Государственные органы и рыночные субъекты используют сбор и обработку данных для повышения эффективности своей деятельности, однако при этом граждане всё чаще теряют фактический контроль над собственной информацией. Развитие технологий больших данных и интернет-технологий сопровождается новыми формами нарушения прав на личную информацию. В этих условиях одних только гражданско-правовых и уголовно-правовых средств защиты недостаточно для полноценного реагирования на возникающие риски. Поэтому публично-правовое обеспечение безопасности персональных данных следует рассматривать как необходимый комплексный механизм, позволяющий защищать персональные данные на различных стадиях их обработки и учитывать особенности цифровой эпохи.

Подводя итог параграфу и главе в целом, можно сформулировать следующие выводы. В условиях стремительного развития цифровых технологий в Китае и России, увеличения количества утечек персональных данных необходимо развитие системы административно-правового и информационно-правового

---

[421] *Ван Гуанлун.* Административно-правовые меры по обеспечению безопасности персональных данных при раскрытии информации правительством в Китае. // Вестник Санкт-Петербургского университета. Право. 2024. № 3. С. 815-834.

обеспечения безопасности персональных данных, включая следующие меры: конкретизацию иерархических взаимосвязей между нормативными правовыми актами при их применении [422] ; интеграцию ресурсов сетевого контроля с внедрением современных технологий больших данных, включая разработку комплексной платформы для мониторинга обработки персональных данных и совершенствование механизма контроля и надзора в целях обеспечения безопасности персональных данных; совершенствование системы административной поддержки для защиты персональных данных, а также усиление развития судебной защиты прав на персональные данные в интересах субъектов персональных данных и общества. Обоснована необходимость развития законодательства об административных правонарушениях в части обновления и уточнения составов административных правонарушений, в том числе с позиции дифференциации правонарушений и ответственности в зависимости от оператора персональных данных.

В целях обеспечения безопасности персональных данных при открытии государственных данных обоснована необходимость развития следующих мер: мер по обеспечению соблюдения баланса общественных интересов и законных интересов физических лиц в области защиты персональных данных на основе принципа соразмерности; мер по созданию и улучшению системы правового регулирования обеспечения доступности и открытого использования государственных данных[423]; мер по созданию механизма оценки рисков в сфере открытия государством данных с целью улучшения системы обработки органами исполнительной власти персональных данных.

Российский и китайский подходы к правовому регулированию персональных данных демонстрируют различные методологические парадигмы, сформированные национальными правовыми традициями. В России доминирует информационно-правовая модель, основу которой составляют акты информационного законодательства (Федеральный закон «О персональных

[422] *Ван Гуанлун.* Административно-правовая защита персональной информации в Китае: недостатки и путь решения // Вестник Университета имени О.Е. Кутафина (МГЮА). 2024. № 10. С. 189-197.
[423] *Ван Гуанлун.* Административно-правовая защита персональной информации в Китае: недостатки и путь решения // Вестник Университета имени О.Е. Кутафина (МГЮА). 2024. № 10. С. 189-197.

данных» и другие нормативные правовые акты), направленные на обеспечение безопасности персональных данных. В Китае сохраняется приоритет административно-правового регулирования, интегрирующего защиту данных в систему государственного управления, с постепенным включением элементов формирующегося цифрового законодательства. Несмотря на разную отраслевую доминанту, оба подхода носят межотраслевой характер: российская система реализуется через взаимодействие специальных информационно-правовых и конституционных, административных, уголовно-правовых, гражданско-правовых мер обеспечения безопасности персональных данных, в то время как китайская модель сочетает конституционные основы и административный контроль с развивающимися частноправовыми инструментами в цифровой сфере. Это отражает общую тенденцию к комплексному регулированию персональных данных в условиях цифровой трансформации.

Установлено, что академическая институционализация исследований в области публично-правовой защиты персональных данных обусловлена во многом тем, что в России информационное право консолидировалось как комплексная отрасль права и самостоятельная отрасль юридической науки с оформлением отдельного предметного поля, созданием профильных кафедр и образовательных программ в ведущих юридических вузах. В Китае, несмотря на официальный статус в системе юридических дисциплин, «информационное право» развивается преимущественно в междисциплинарном режиме в рамках традиционных кафедр, что указывает на продолжающийся процесс его научно-образовательной институционализации как самостоятельной юридической науки и учебной дисциплины. Эти различия иллюстрируют более широкие дивергентные траектории адаптации разных правовых механизмов обеспечения безопасности персональных данных к вызовам цифровой трансформации. Данное различие обусловлено как особенностями правовых традиций двух государств, так и определёнными отличиями стратегических приоритетов развития в России и Китае. При том выявлено, что правовые системы России и Китая в части публично-правового обеспечения безопасности персональных данных

демонстрируют тенденцию к конвергенции, адаптируясь к вызовам цифровой трансформации посредством развития межотраслевых механизмов правового регулирования персональных данных и публично-правового обеспечения их безопасности.

При сопоставлении институциональных моделей публично-правового обеспечения безопасности персональных данных в Китае и России выявлены различные системные подходы, детерминированные национальными административными и правовыми традициями. Китайская модель характеризуется сетевым (полицентричным) регулированием с распределением компетенций между Центральным комитетом по вопросам киберпространства, Министерством промышленности и информатизации и Министерством общественной безопасности. Российская модель, напротив, воплощает функционально-концентрированную парадигму, где ключевые полномочия закреплены за Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации, Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), Федеральной службой безопасности Российской Федерации (ФСБ России) – в части установления требований к защите информации в государственных информационных системах и использования средств криптографической защиты и Федеральной службой по техническому и экспортному контролю (ФСТЭК России) – в части установления требований по защите информации ограниченного доступа от несанкционированного доступа.

# ЗАКЛЮЧЕНИЕ

Результаты диссертационного исследования демонстрируют, что вопрос совершенствования мер по публично-правовому обеспечению безопасности персональных данных граждан в Китае и России является одним из ключевых применительно к правовому обеспечению информационной безопасности. Указанное обстоятельство объясняется тем, что правонарушения в сфере персональных данных в Китае и России становятся всё более чувствительными для общества и затрагивают широкий круг основных прав и свобод человека. Рост числа таких нарушений отрицательно влияет на доверие граждан к действенности правовой защиты в цифровой среде. Хотя Россия и Китай уже приняли специальные законодательные акты, а практика их применения постепенно расширяется, статистика зарегистрированных административных правонарушений в этой области по-прежнему демонстрирует увеличение.

Результаты проведённого диссертационного исследования дают основание сформулировать следующие выводы.

1. В законодательстве Китая и России идентифицируемость рассматривается как один из основных признаков персональных данных. Именно она позволяет определить, в каких случаях информация нуждается в правовой защите, а когда её использование может считаться допустимым и разумным. В то же время персональные данные обладают и другими особыми свойствами, обусловленными их различным содержанием и формами, включая чувствительность, конфиденциальность и социальность. «Идентификация» признается наиболее важным юридическим атрибутом персональной информации и рассматривается как необходимый элемент для ее защиты; только «идентифицируемая» или «идентифицированная» информация напрямую связана с нанесением ущерба личной информации или интересам конфиденциальности. Под «чувствительностью» персональной информации следует понимать вероятность того, что её обработка и использование могут повлечь угрозы или существенный вред для субъекта данных. С точки зрения субъекта персональных данных данная

категория отражает не только объективный уровень риска, но и ограниченность возможностей лица контролировать дальнейшее обращение со сведениями о себе. Поскольку персональные данные в соответствии с законодательством относятся к информации ограниченного доступа, они требуют специальной защиты, а их обработка должна обеспечивать конфиденциальность. Нарушение режима защиты таких данных может привести к тяжёлым последствиям, в том числе к незаконному использованию личности, мошенническим действиям и вмешательству в частную жизнь.

Технологии больших данных позволяют по-новому оценить социальное значение персональных данных. Сегодня персональная информация всё чаще рассматривается не только как объект индивидуальной защиты, но и как ресурс, использование которого при соблюдении правовых требований может отвечать как частным, так и общественно значимым потребностям.

Сравнительный анализ правовой природы персональных данных в Китае и России выявляет как сходные элементы, так и принципиальные различия. Общим для двух правопорядков является признание особых свойств персональных данных — чувствительности, конфиденциальности и социальной значимости, обусловленных разнообразием содержания и форм выражения такой информации. Различия связаны главным образом с критериями, по которым определяется предел правовой охраны. В китайском подходе таким критерием выступает идентифицируемость лица, включая прямую и косвенную идентификацию; через него проводится граница между защищаемой персональной информацией и сферой её правомерного использования. Российское законодательство, закрепляя персональные данные как «любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу», формально использует сопоставимый широкий критерий, поскольку также связывает правовой режим данных с их отношением к конкретному физическому лицу. Ключевое различие заключается не в абсолютной «широте» определения, а в системообразующем значении, которое придается этому критерию в правоприменительной практике, а также в методах его интерпретации

контрольно-надзорными и судебными органами. Таким образом, российский подход потенциально формирует более широкое концептуальное поле для отнесения информации к персональным данным, что создает дополнительные гарантии защиты прав личности, но одновременно может порождать большую степень неопределенности в правоприменении, например, при определении применимости требований по обеспечению безопасности к тем или иным данным, имеющим признаки персональных.

2. В Законе КНР о ПДн персональные данные делятся на чувствительную и обычную личную информацию, а также на этой основе определяются специальные правила обработки чувствительной персональной информации, что соответствует тенденциям развития законодательства о персональных данных в большинстве государств мира и позволяет более эффективно предотвращать риски, связанные с персональной информацией. Установлено, что степень чувствительности личной информации зависит не только от её внутренних характеристик, но и от специфики и условий конкретного сценария (цели) её использования и совершения иных действий. Основная цель обеспечения безопасности персональных данных заключается в гарантировании защищенности прав и законных интересов субъектов персональных данных, в минимизации рисков, связанных с их использованием и совершением иных действий с ними, в том числе в предотвращении возможных негативных последствий таких действий, а также восстановление нарушенных прав. Для адаптации к особенностям определения чувствительной личной информации, основанного на контексте конкретных сценариев (целей), рекомендуется внедрение разработанного системного подхода к обеспечению безопасности данных, подразумевающего внедрение публично-правовых мер, основанных на соответствующих правовых толкованиях, административных регламентах и отраслевых правилах. Выявлено, что такая динамическая дифференциация способствует повышению предсказуемости и эффективности обработки данных, оптимизации корпоративного комплаенса и связанных с ним затрат, что, в свою очередь, создает благоприятные условия для развития экономики данных. Также

выявлены особенности и сделаны предложения в части российского подхода к категорированию персональных данных.

3. На основе доктринальных положений о достоинстве личности и институте персональных данных, теоретического содержания прав и свобод человека, а также анализа их природы и ключевых принципов, с учетом норм международных документов и национальных конституций, была разработана ценностная основа правовой защиты персональных данных, представляющая собой уважение к человеческому достоинству и обеспечение информационной свободы.

4. Установлено, что теоретической основой защиты персональных данных как в России, так и в Китае выступает механизм обеспечения баланса интересов. В Китае он концептуализирован в рамках «персональной кибернетики» и «социальной кибернетики», в России – в форме принципа баланса интересов личности, общества и государства, активно реализуемого в системе правового обеспечения информационной безопасности. Данный механизм направлен на определение, выявление и защиту прав и законных интересов граждан, связанных с персональными данными, с использованием комплекса правовых средств.

В целях повышения эффективности данного механизма представляется необходимым дальнейшее развитие и конкретизация системы действующих принципов правового регулирования персональных данных в обоих государствах через призму задачи обеспечения баланса. В рамках данного подхода баланс интересов участников отношений в сфере персональных данных следует рассматривать не только как отдельный принцип, но и как общий ориентир для применения других правовых начал, таких как законность, справедливость, соразмерность, целевое ограничение, минимизация данных. Такой подход может способствовать дальнейшему совершенствованию нормативного регулирования, поскольку позволяет одновременно учитывать приоритет человеческого достоинства, общественные и государственные интересы, а также предупреждать возможные конфликты между различными субъектами в процессе обеспечения безопасности и защиты персональных данных.

Таким образом, научный и практический акцент переносится с формального

закрепления самостоятельного принципа баланса на исследование взаимосвязи конкретных правовых принципов и механизмов, обеспечивающих его достижение в национальных системах безопасности персональных данных.

5. В рамках информационно-правового обеспечения безопасности персональных данных представляется возможным рассматривать право на персональные данные как самостоятельный вид субъективного права. Вместе с тем такое понимание требует уточнения его связи с правом на защиту персональных данных, уже закрепившимся в российской доктрине и практике как производным от права на неприкосновенность частной жизни. Предлагаемая конструкция не противопоставляется существующему подходу, а дополняет его в условиях цифровой трансформации. Её смысл заключается в переходе от преимущественно пассивной модели защиты к признанию за лицом активного правомочия распоряжаться своими данными и контролировать их использование в установленных законом пределах. Ценность данного подхода состоит в создании более гибкой и технологически нейтральной теоретической основы для механизма обеспечения безопасности персональных данных.

Во-первых, хотя абсолютный индивидуальный контроль над информацией (информационное самоопределение) не всегда соответствует природе информационного обмена, признание за субъектом определённого объёма правомочий по контролю и участию в процессах обработки его данных является необходимым. Во-вторых, данная концепция отличается гибкостью, позволяющей учитывать динамику современного развития технологий и обеспечивать защиту достоинства личности в новых условиях цифровой среды.

При формировании китайской и российской моделей информационного права определение места этого права в системе правоотношений влияет на создание целостного механизма защиты. В контексте системы субъективных прав в информационной сфере предлагается рассматривать право на персональные данные как правомочие, производное не только от охраны человеческого достоинства, но и от совокупности конституционных ценностей: неприкосновенности частной жизни, личной и семейной тайны, права

на свободное развитие личности и защиты от произвольного вмешательства. Такой подход позволяет сбалансированно сочетать защиту прав субъектов данных с потребностями информационного общества, обеспечивая системное развитие информационного права.

6. Исследование принципов обработки персональных данных в России и Китае позволило обосновать, что принципы обработки персональных данных выступают одной из базовых публично-правовых мер обеспечения безопасности персональных данных как в Российской Федерации, так и в Китайской Народной Республике. Они представляют собой совокупность идей, начал, универсально распространяемых на все отношения, складывающиеся в сфере обработки персональных данных, а также оказывающих непосредственное влияние на законодательство о персональных данных и правоприменительную практику в сфере обеспечения безопасности персональных данных. Установлено, что в качестве самостоятельного принципа обработки персональных данных в России необходимо рассматривать принцип обеспечения конфиденциальности персональных данных (в Китае он обозначен как принцип обеспечения безопасности).

Данный принцип обеспечивает реализацию главной особенности персональных данных как вида информации ограниченного доступа – распространение на них режима конфиденциальности и необходимости его соблюдения, независимо от того, были ли они раскрыты субъектом персональных данных или нет. Он предполагает недопустимость утраты конфиденциальности персональных данных, влияет на развитие законодательства о персональных данных в части обеспечения их конфиденциальности, а также оказывает воздействие на правоприменение при разрешении конкретных споров в сфере персональных данных.

7. По результатам исследования в работе обосновано, что в условиях стремительного развития цифровых технологий в Китае и России, увеличения количества утечек персональных данных необходимо развитие системы административно-правового и информационно-правового обеспечения

безопасности персональных данных, включая следующие меры: конкретизацию иерархических взаимосвязей между нормативными правовыми актами при их применении; интеграцию ресурсов сетевого контроля с внедрением современных технологий больших данных, включая разработку комплексной платформы для мониторинга обработки персональных данных и совершенствование механизма контроля и надзора в целях обеспечения безопасности персональных данных; совершенствование системы административной поддержки для защиты персональных данных, а также усиление развития судебной защиты прав на персональные данные в интересах субъектов персональных данных и общества. Обоснована необходимость развития законодательства об административных правонарушениях в части обновления и уточнения составов административных правонарушений, в том числе с позиции дифференциации правонарушений и ответственности в зависимости от оператора персональных данных.

В целях обеспечения безопасности персональных данных при открытии государственных данных обоснована необходимость развития следующих мер: меры по обеспечению соблюдения баланса общественных интересов и законных интересов физических лиц в области защиты персональных данных на основе принципа соразмерности; создание и улучшение системы правового регулирования обеспечения доступности и открытого использования государственных данных; создание механизма оценки рисков в сфере открытия государством данных с целью улучшения системы обработки органами исполнительной власти персональных данных.

8. Выявлено, что российский и китайский подходы к правовому регулированию персональных данных демонстрируют различные методологические парадигмы, сформированные национальными правовыми традициями. В России доминирует информационно-правовая модель, основу которой составляют акты информационного законодательства (Федеральный закон «О персональных данных» и другие нормативные правовые акты), направленные на обеспечение безопасности персональных данных. В Китае сохраняется приоритет административно-правового регулирования, интегрирующего защиту

данных в систему государственного управления, с постепенным включением элементов формирующегося цифрового законодательства. Несмотря на разную отраслевую доминанту, оба подхода носят межотраслевой характер: российская система реализуется через взаимодействие специальных информационно-правовых и конституционных, административных, уголовно-правовых, гражданско-правовых мер обеспечения безопасности персональных данных, в то время как китайская модель сочетает конституционные основы и административный контроль с развивающимися частноправовыми инструментами в цифровой сфере. Это отражает общую тенденцию к комплексному регулированию персональных данных в условиях цифровой трансформации.

Установлено, что академическая институционализация исследований в области публично-правовой защиты персональных данных обусловлена во многом тем, что в России информационное право консолидировалось как комплексная отрасль права и самостоятельная отрасль юридической науки с оформлением отдельного предметного поля, созданием профильных кафедр и образовательных программ в ведущих юридических вузах. В Китае информационное право, несмотря на его признание в системе юридических дисциплин, пока развивается преимущественно в междисциплинарной форме и чаще всего остаётся связанным с традиционными кафедрами. Поэтому его институционализация как самостоятельной юридической науки и учебной дисциплины ещё не может считаться завершённой. В этом проявляется одно из различий между китайским и российским подходами к адаптации правовых механизмов защиты персональных данных к условиям цифровой трансформации. Такое различие объясняется как национальными правовыми традициями, так и разными акцентами в стратегическом развитии двух государств. Однако наряду с этим можно отметить и сближение двух систем: в обеих странах усиливается публично-правовой компонент защиты персональных данных, развиваются межотраслевые механизмы регулирования и расширяется набор гарантий, направленных на обеспечение их безопасности.

9. При раскрытии государственных данных, включающих персональные

сведения, защита прав граждан должна рассматриваться наряду с публичным интересом в доступе к информации и задачами устойчивого развития общества. Для этого необходимы меры, ориентированные не только на последующее привлечение к ответственности, но и на предупреждение нарушений со стороны операторов. В частности, регулярный комплаенс-аудит в сфере персональных данных может использоваться как инструмент проверки соблюдения законодательства и раннего выявления рисков. Повышение строгости административных санкций, в свою очередь, усиливает значение внутренних процедур комплаенса и побуждает операторов ответственнее подходить к обеспечению безопасности персональных данных.

Также необходимо создание механизма оценки рисков для государственных данных с целью совершенствования системы обработки личной информации органами исполнительной власти может быть структурировано следующим образом:

- субъекты обработки информации должны определить необходимость проведения оценки рисков в соответствии с установленными методологическими принципами и критериями;

- уполномоченные подразделения по защите персональных данных на всех уровнях власти осуществляют детальную оценку рисков, принимая во внимание предполагаемый уровень угроз и масштаб воздействия;

- органы государственной власти, ответственные за защиту персональных данных, обязаны подготовить комплексные отчеты об оценке рисков, содержащие подробный анализ потенциальных угроз нарушения конфиденциальности гражданских данных и предложения по эффективным мерам их минимизации;

- субъекты обработки информации должны использовать результаты анализа рисков для принятия решений по управлению соответствующими административными проектами, обеспечивая их соответствие установленным требованиям безопасности.

10. При сопоставлении институциональных моделей публично-правового обеспечения безопасности персональных данных в Китае и России выявлены

различные системные подходы, детерминированные национальными административными и правовыми традициями. Китайская модель характеризуется сетевым (полицентричным) регулированием с распределением компетенций между Центральным комитетом по вопросам киберпространства, Министерством промышленности и информатизации и Министерством общественной безопасности. Российская модель, напротив, воплощает функционально-концентрированную парадигму, где ключевые полномочия закреплены за Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации, Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), Федеральной службой безопасности Российской Федерации (ФСБ России) – в части установления требований к защите информации в государственных информационных системах и использования средств криптографической защиты и Федеральной службой по техническому и экспортному контролю (ФСТЭК России) – в части установления требований по защите информации ограниченного доступа от несанкционированного доступа.

# СПИСОК СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

ГК КНР — Гражданский кодекс Китайской Народной Республики

ГОСОПКА — Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак

ЕС — Европейский союз

Закон КНР о ПДн — Закон Китайской Народной Республики о защите персональных данных

КНР — Китайская Народная Республика

Конвенция Совета Европы от 1981 года — Конвенция о защите физических лиц в отношении автоматической обработки персональных данных, принятой Европейской комиссией в 1981 году

Конституция КНР — Конституция Китайской Народной Республики

Конституция РФ — Конституция Российской Федерации

КС РФ — Конституционный Суд Российской Федерации

КоАП РФ — Кодекс Российской Федерации об административных правонарушениях

КИИ — Критическая информационная инфраструктура

ПК ВСНП — Постоянный комитет Всекитайского собрания народных представителей

РФ — Российская Федерация

Роскомнадзор — Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций

США — Соединённые Штаты Америки

ФЗ о ПДн — Федеральный Закон от 27 июля 2006г. № 152-ФЗ «О персональных данных»

ФСБ России — Федеральной службой безопасности Российской Федерации

ФСТЭК России — Федеральной службы по техническому и экспортному контролю

ЦК КПК — Центральный комитет Коммунистической партии Китая

GDPR — Общий регламент по защите данных, законодательный акт Европейского Союза

SAMR — Государственная администрация по регулированию рынка Китая

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

## 1. Основные нормативные правовые акты в Китае и России

### 1.1. Нормативные правовые акты Российской Федерации

*Конституция, федеральные законы, законы субъектов Российской Федерации:*

1. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 года с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 года) // Официальный интернет-портал правовой информации http://pravo.gov.ru, 06.10.2022.

2. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ // Собрание законодательства РФ. 1994. № 32. Ст. 3301.

3. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ // Собрание законодательства РФ. 2001. № 2002. № 1 (1 ч.). Ст. 1.

4. Федеральный закон от 30 ноября 2024 г. № 420-ФЗ«О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» // Собрание законодательства РФ. 2024. № 49 (4 ч.). Ст. 7411.

5. Федеральный закон от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» // Собрание законодательства РФ. 2023. № 1 (ч. 1). Ст. 19.

6. Федеральный закон от 14.07.2022 № 266-ФЗ «О внесении изменений в Федеральный закон «О персональных данных», отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона «О банках и банковской деятельности» // Собрание законодательства РФ. 2022. № 29 (ч. III). Ст. 5233.

7. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства РФ. 2017. № 31 (1 ч.). Ст. 4736.

8. Федеральный закон от 21.07.2014 № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно телекоммуникационных сетях» // Российская газета. 2014. № 163.

9. Федерального закона «Об основах охраны здоровья граждан в Российской Федерации»: // Собрание законодательства РФ. 2011 . №48. Ст. 6724.

10. Федеральный закон от 25.07.2011 № 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» // Собрание законодательства РФ. 2011. № 31. Ст. 4701

11. Федеральный закон от 9 февраля 2009 г. №8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» // Собрание законодательства РФ. 2009. № 7 (1 ч.). Ст. 776.

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

13. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3448.

*Указы Президента Российской Федерации, постановления и распоряжения Правительства Российской Федерации:*

14. Указ Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства РФ. 2021. № 27( 2 ч.). Ст. 5351.

15. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ. 2016. № 50. Ст. 7074.

16. Указ Президента РФ от 30 апреля 2005 № 609 «Об утверждении Положения о персональных данных государственного служащего Российской Федерации и ведения его личного дела» // Собрание законодательства РФ. 2005. № 23. Ст. 2242.

17. Постановление Правительства РФ от 16 января 2023 № 24 «Об утверждении Правил принятия решения уполномоченным органом по защите прав субъектов персональных данных о запрещении или об ограничении трансграничной передачи персональных данных в целях защиты нравственности, здоровья, прав и законных интересов граждан» // Собрание законодательства РФ. 2023. № 4. Ст. 644.

18. Постановление Правительства РФ от 10 января 2023 № 6 «Об утверждении Правил принятия решения о запрещении или об ограничении трансграничной передачи персональных данных уполномоченным органом по защите прав субъектов персональных данных и информирования операторов о принятом решении» // Собрание законодательства РФ. 2023. № 3. Ст. 122.

19. Постановление Правительства РФ от 16 июня 2022 № 1089 «Об утверждении Положения о единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица» // Собрание законодательства РФ. 2022. № 26. Ст. 4163.

20. Постановление Правительства РФ от 13 февраля 2019 № 146 «Об утверждении Положения о государственном контроле и надзоре за соответствием обработки персональных данных требованиям законодательства Российской Федерации» // Собрание законодательства РФ. 2019. № 7 (2 ч.). Ст. 673.

21. Постановление Правительства РФ от 15 апреля 2014 № 313 «Об утверждении государственной программы Российской Федерации «Информационное общество» // Собрание законодательства РФ. 2014. № 18 (2 ч.). Ст. 2159.

22. Постановление Правительства РФ от 10.07.2013 г. № 583 «Об обеспечении доступа к общедоступной информации о деятельности государственных органов и органов местного самоуправления в информационно-телекоммуникационной сети «Интернет» в форме открытых данных» // Собрание законодательства РФ. 2013. № 30. Ст. 4107.

23. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собрание законодательства РФ. 2012. № 45. Ст. 6257.

24. Постановление Правительства РФ от 21 марта 2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» // Собрание законодательства РФ. 2012. № 14. Ст. 1626.

25. Постановление Правительства РФ от 01 ноября 2012 № 1119 «Об утверждении требований к за щите персональных данных при их обработке в информационных системах персональных данных» // Собрание законодательства РФ. 2012. № 45. Ст. 6257.

*Нормативные правовые и иные акты органов исполнительной власти:*

26. Приказ Роскомнадзора от 27 октября 2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»» // СПС «КонсультантПлюс».

27. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.08.2022 № 128 «Об утверждении перечня иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных» // Собрание законодательства РФ. 2022. № 16. Ст. 967.

28. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 30.05.2017 № 94 «Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения». [Электронный ресурс]. Режим доступа: https://www.garant.ru/products/ipo/prime/doc/71652212/?ysclid=lwchijkaii571205726, свободный (дата обращения: 01.06.2025).

*Материалы судебной практики*

29. Решение Арбитражного суда г.Москвы от 5 марта 2026 г. по делу N А40-351064/2025 // СПС «Гарант».

30. Решение Арбитражного суда г.Санкт-Петербурга и Ленинградской области от 10 марта 2026 г. по делу № А56-4733/2026 // СПС «Гарант».

31. Определение Верховного Суда РФ от 08.09.2020 № 308-ЭС20-11154 по делу № А63-13382/2019 // СПС «Гарант».

32. Постановление Второго арбитражного апелляционного суда от 08.08.2019 № 02АП-5517/2019 по делу № А31-3955/2019 // СПС «Гарант».

33. Определение Московского городского суда от 13.05.2019 № 4г-4164/19 // СПС «Гарант».

34. Решение Октябрьского районного суда г. Белгорода от 12 сентября 2019 г. по делу № 12-393/2019 // СПС «Гарант».

35. Постановление Седьмого арбитражного апелляционного суда от 05.04.2018 № 07АП-1437/2018 по делу № А45-31682/2017 // СПС «Гарант».

36. Определение Судебной коллегии по гражданским делам Верховного Суда РФ от 01.08.2017 № 78-КГ17-45 // СПС «Гарант».

37. Постановление Восемнадцатого арбитражного апелляционного суда от 05.04.2017 № 18АП-2210/2017 по делу № А07-24090/2016 // СПС «Гарант».

38. Апелляционное определение Санкт-Петербургского городского суда от 03.02.2015 № 33- 1644/2015 по делу № 2-3097/2014 // СПС «Гарант».

### 1.2. Нормативные правовые акты Китайской Народной Республики

*Конституция, законы Китайской Народной Республики:*

39. Конституция Китайской Народной Республики. Принята в 1982 году, вступила в силу в том же году. Последняя (пятая) редакция принята в 2018 году. URL: http://www.npc.gov.cn/npc/c191/c505/201905/t20190521_263492.html (дата обращения: 31.10.2025)

40. Закон КНР о защите персональной информации. Принят 20 августа 2021 года, вступил в силу 1 ноября 2021 года. URL: http://www.npc.gov.cn/c2/c30834/202108/t20210820_313088.html (дата обращения: 31.10.2025)

41. Закон КНР о безопасности данных. Принят 10 июня 2021 года, вступил в силу 1 сентября 2021 года. URL: http://www.npc.gov.cn/npc/c2/c30834/202106/t20210610_311888.html (дата обращения: 31.10.2025)

42. Закон КНР о кибербезопасности. Принят 7 ноября 2016 года, вступил в силу 1 июня 2017 года. URL: https://www.cac.gov.cn/2016-11/07/c_1119867116.htm (дата обращения: 31.10.2025)

43. Закон КНР о социальном страховании. Принят 28 октября 2010 года, вступил в силу 1 июля 2011 года. Пересмотрен 29 декабря 2018 года. URL: http://www.npc.gov.cn/zgrdw/npc/xinwen/2019-01/07/content_2070267.htm (дата обращения: 31.10.2025)

44. Закон КНР об административном пересмотре. Принят 29 апреля 1999 года, вступил в силу 1 октября 1999 года. Последняя редакция завершена 1 сентября 2023 года и вступила в силу 1 января 2024 года. URL: https://www.gov.cn/yaowen/liebiao/202309/content_6901584.htm (дата обращения: 31.10.2025)

45. Закон КНР об административных наказаниях. Принят 17 марта 1996 года, вступил в силу 1 октября 1996 года. Пересмотрен в 2021 году. URL: http://www.npc.gov.cn/npc/c2/c30834/202101/t20210122_309857.html (дата обращения: 31.10.2025)

46. Закон КНР о защите прав и интересов потребителей. Принят 31 октября 1993 года. Пересмотрен 25 октября 2013 года, редакция вступила в силу

15 марта 2014 года. URL: https://www.samr.gov.cn/zt/ndzt/2019n/bjspjsqjxcjwljxyjsckpxc/zcfg/art/2023/art_5004b2b0f4154c76acfca499fe9c737a.html (дата обращения: 31.10.2025)

**2. Книги (монографии, учебники, учебные пособия)**

**2.1. Специальная научная литература на русском и китайском языках**

47. Авакьян С. А. Конституционное право России. Учебный курс: Учеб. пособие: В 2 т. 5-е изд., перераб. и доп. М.: Норма, 2014. Т. 1. 863 с.

48. Алешкова И. А., Андриченко Л. В., Умнова И. А. Конституционное право Российской Федерации: В 2 т. М.: Юрайт, 2015. Т. 2. 439 с.

49. Алита Л. Аллен, Ричард К. Стоктон. Право на неприкосновенность частной жизни в США: доктрина, прецедент и законодательство. Перевод: Фэн Цзяньмэй и др. Пекин: Издательство "Китайская демократия и право", 2019. 400 с.

50. Бачило И.Л. Информационное право / И.Л. Бачило, В.Н. Лопатин, М.А. Федотов. СПб.: Юридический центр Пресс, 2005. 789 с.

51. Бачило И.Л., Сергиенко Л.А., Кристальный Б.В., Арешев А.Г. Персональные данные в структуре информационных ресурсов. Основы правового регулирования. Минск, 2006. 473 с.

52. Ван Жун. Защита данных и правила их передачи в эпоху больших данных. Пекин: Народное издательство "почта и телекоммуникации", 2017. 293 с.

53. Ван И. Конституционализм. Трансформация концепций и систем. – Цзинань: Народное издательство Шаньдуна, 2006. 478 с.

54. Ван Лимин. Законы о правах личности. Пекин: Издательство Китайского народного университета, 2005. 780 с.

55. Волчинская Е.К. Защита персональных данных. Опыт правового регулирования. М.: Галерея, 2001. 236 с.

56. Гегель. Основы философии права. Перевод: Фань Ян, Чжан Цитай. Пекин: Коммерческая пресса, 1961. 360 с.

57. Джингте Якобус. Норма. Личность. Общество – предпосылки права философии [М]. Перевод Фэн Цзюня, Пекин: Юридическая пресса, 2001. 137 с.

58. Джон Ролс. Теория справедливости. Перевед: Хэ Хуайхун и др. Пекин: Издательство китайских общественных наук, 1988. 627 с.

59. Дин Сяодун. Защита личной информации: принципы и практика. Пекин: Юридическое издательство, 2021. 321 с.

60. Ду Чэнмин. Улучшение и реконструкция: Исследование основных прав в период социальных трансформаций. Пекин: Издательство Китайского политико-юридического университета, 2012. 422 с.

61. Избранные нормативно-правовые акты Китайской Народной Республики в области цифровизации / пер. с кит Ли Яо. М.: Проспект, 2025. 136 с.

62. Иммануил Кант. Критика практического разума. Перевод: Хань Шуйфа. Пекин: Коммерческая пресса, 1999. 200 с.

63. Кудж С.А. Информационное поле: Монография. М.: МАКС Пресс, 2017. 97 с.

64. Лян Шаншан. Теория затрат и выгод. Пекин: Издательство Пекинского университета, 2021. 352 с.

65. Ли Яо. Избранные нормативно-правовые акты Китайской Народной Республики в области цифровизации. – М.: Проспект, 2025. – 136 с.

66. Ма Яньсинь, Ли Чжэ, Юань Цян и др. Цифровое правительство: перемены и верховенство закона. Пекин: Издательство Китайского университета Жэньминь, 2021. 388 с.

67. Малеина М. Н. Личные неимущественные права граждан: понятие, осуществление, защита. М.: МЗ-Пресс, 2000. 242 с.

68. Монтескье. О духе законов (часть 1). Перевод: Сюй Минлун. Пекин: Коммерческая пресса, 2012. 759 с.

69. Морозов А.В., Филатова Л.В., Полякова Т.А. Информационное право и информационная безопасность. Часть 2. Учебник. М.: РПА, 2016. 604 с.

70. Морозов А.В., Филатова Л.В. Правовые вопросы доступа к информации. Учебное пособие. М.: РПА, 2015. 82 с.

71. Назаров Д.М. Основы обеспечения безопасности персональных данных в организации: учеб. Пособие / Д.М. Назаров, К.М. Саматов; М-во науки и

высш. Образования Рос. Федерации, Урал. гос. экон. ун-т. Екатеринбург: Изд-во Урал. гос. экон. ун-та, 2019. 118 с.

72. Петрухин И. Л. Личные тайны (человек и власть). М.: Институт государства и права РАН, 1998. 230 с.

73. Право персональных данных: учебник / под об. ред. д.ю.н., профессора А.В. Минбалеева. Саратов: ООО «Амирит», 2023. 415 с.

74. Право персональных данных : учебник / под ред. д-ра юрид. наук, профессора А. В. Минбалеева. 2-е изд., доп. и перераб. М.: Издательский центр Университета имени О.Е. Кутафина (МГЮА), 2025. 320 с.

75. Романовский Г. Б. Право на неприкосновенность частной жизни. М.: МЗ-Пресс, 2001. 309 с.

76. Рональд Дворкин. О правах всерьёз. Перевод: Синь Чуньин, Ву Юйчжан. Шанхай: Книжный магазин "Саньлянь", 2008. 389 с.

77. Руссо. Общественный договор. Перевод: Ли Пин-оу. Пекин: Коммерческая пресса, 2011. 176 с.

78. Фридрих фон Хайек. Индивидуализм и экономический порядок. Перевед: Цзя Чжань и др. Пекин: Издательство Пекинского экономического института, 1989. 188 с.

79. Хань Дэцян. О человеческом достоинстве: интерпретация теории человеческого достоинства с точки зрения права. Пекин: Юридическая пресса, 2009. 350 с.

80. Чжан Синьбао. Правовая защита права на неприкосновенность частной жизни. Пекин: Издательство "Массы", 2004. 394 с.

81. Чжоу Ханьхуа. Закон Китайской Народной Республики о защите персональной информации (проект рекомендаций экспертов) и отчет об исследовании законодательства. Пекин: Юридическая пресса, 2006. 104 с.

82. Эбзеев Б. С. Введение в Конституцию России. М.: Норма: ИНФРА-М, 2013. 559 с.

83. Юй Вэньхао. Основные права. Нанкин: Цзянсуский народное издательство, 2016. 212 с.

### 2.2. Статьи, периодические издания на русском и китайском языках

84. Арановский К., Князев С. Роль конституции в политико-правовом обустройстве России: исходные обстоятельства и современные ожидания // Сравнительное конституционное обозрение. 2013. № 3. С. 50-59.

85. Балашкина И.В. Особенности конституционного регулирования права на неприкосновенность частной жизни в Российской Федерации // Право и политика. 2007. № 7. С. 92-105.

86. Бундин М.В. Опыт правового регулирования права на частную жизнь и персональных данных в Соединенных Штатах Америки // Журнал зарубежного законодательства и сравнительного правоведения. 2012. № 3. С. 162-168.

87. Важорова М. А. История возникновения и становления института персональных данных // Государство и право: теория и практика: материалы I Междунар. науч. конф. (г. Челябинск, апрель 2011 г.). Челябинск: Два комсомольца, 2011. С. 33-38.

88. Важорова М.А. Соотношение понятий «информация о частной жизни» и «персональные данные» // Вестник Саратовской государственной юридической академии. 2012. № 4 (87). С. 55-59.

89. Ван Кай. Защита основных прав в доступе к записям звонков (сообщений) // Политика и право. 2020. № 8. С. 107-119.

90. Ван Кай. Конституционная основа для кодификации Экологического кодекса // Юридические обзоры. 2022. № 5. С. 174-186.

91. Ван Кай. Об общих правах личности, закрепленных в Конституции, и их влияние на гражданское право // Юридическая наука в Китае. 2017. № 3. С. 102-121.

92. Ван Лэй. Достижения и проблемы, связанные с конституционными гарантиями основных прав граждан // Гуандунские общественные науки. 2013. № 3. С. 221-229.

93. Ван Сигэнь. Ценность прав человека в представлении Си Цзиньпина о верховенстве закона // Восточное право. 2021. № 1. С. 37-46.

94. Ван Сисинь. Национальные обязательства по защите персональной информации и их разъяснение // Юридическая наука в Китае. 2021. № 1. С. 145-166.

95. Ван Сицзинь, Пэн Чжунь. Конституционная основа правовой системы защиты персональной информации // Цинхуаское право. 2021. № 3. С. 6-24.

96. Ван Сюй. Теория достоинства в конституционном праве и ее систематизация // Китайский юридический журнал. 2016. № 1. С. 37-55.

97. Ван Цзюньсю. Реконструкция концепции неприкосновенности частной жизни в цифровом обществе на примере «распознавания лиц» // Исследования и дискуссия. 2020. № 2. С. 86-90.

98. Ван Чен. Выбор модели гражданско-правовой защиты персональных данных // Китайские общественные науки. 2019. № 6. С. 124-146.

99. Ветров Д.М. Защита персональных данных и защита информации на предприятии. Некоторые спорные вопросы применения // Проблемы права. Челябинск, 2010. № 1. С. 114-121.

100. Ван Гуанлун. Механизм административно-правового регулирования защиты персональных данных в Китае: состояние, недостатки и путь решения // Вестник Московского университета. 2024. Серия 11. Право. Том 65. № 4. С. 204-232.

101. Ван Гуанлун. Административно-правовые меры по обеспечению безопасности персональных данных при раскрытии информации правительством в Китае // Вестник Санкт-Петербургского университета. Право. 2024. № 3. С. 815-834.

102. Ван Гуанлун. Административно-правовая защита персональной информации в Китае: недостатки и путь решения // Вестник Университета имени О.Е. Кутафина (МГЮА). 2024. № 10. С. 189-197.

103. Волчинская Е. Место персональных данных в системе информации ограниченного доступа // Право. Журнал Высшей школы экономики.2014. № 4. 193-207.

104. Гао Фупин, Ли Цюньтао. Новое позиционирование «прав и интересов в сфере персональной информации» в гражданском праве // Труды «Дунюэ». 2023. № 6. С. 166-176.

105. Гао Фупин. Защита персональных данных: от персональной кибернетики к социальной кибернетике // Китайский юридический журнал. 2018. № 3. С. 84-101.

106. Гао Фупин. Основа легитимности использования персональной информации: анализ выгод на данные // Журнал сравнительного правоведения. 2019. № 2. С. 72-85.

107. Гао Чжихун. Юридическая логика и путь оптимизации троичного разделения между неприкосновенностью частной жизни, личной информацией и данными // Правовая система и социальное развитие. 2022. № 2. С. 207-224.

108. Гатиятуллина Э.М. Защита персональных данных в условиях цифровизации: эволюция и современное состояние // Закон и власть. 2023. № 3. С. 33-37.

109. Гиш Т.А., Ржевская Н.В., Медведева А.С. Анализ законодательства разных стран по обеспечению защиты персональных данных // Электронный научный журнал Курского государственного университета. 2023. № 4 (40). https://api-mag.kursksu.ru/api/v1/get_pdf/5181/ (дата обращения: 31.12.2024).

110. Го Даохуэй. Право знать и система раскрытия информации // Цзянхайский академический журнал. 2003. № 1. С. 127-133.

111. Го Минлун. О коммерциализации персональной информации // Юридический форум. 2012. № 6. С. 108-114.

112. Грищенко Г.А. О некоторых актуальных проблемах защиты персональных данных граждан в цифровом пространстве // Аграрное и земельное право. 2025. № 9. С. 143-146.

113. Гуде С.В. Защита персональных данных в Российской Федерации: исторический аспект и современное состояние / С. В. Арбузов, А.Г. Карпика // Юристъ-Правоведъ. 2015. № 2 (69). С. 93-97.

114. Дин Сяодун. Многомерное толкование комплексной защиты персональной информации в рамках публично-частного права // Исследование верховенства права. 2022. № 5. С. 14-25.

115. Дин Сяодун. Размышление и изменение права на личную информацию: применимые предпосылки и основа правовых благ для защиты личной информации // Китайское и иностранное право. 2020. № 2. 339-356

116. Добробаба М.А. Понятие персональных данных: проблема правовой определенности // Вестник университета именно О.Е. Кутафина(МГЮА). 2023. №2. С.44.

117. Ду Цянцян. Доступ суда к записям телефонных разговоров не является проверкой связи в конституционном смысле // Правоведение. 2019. № 12. С. 78-87.

118. Дудко М.О. Понятие "персональные данные" в современном праве // Вестник Гродненского государственного университета имени Янки Купалы. Серия 4. 2020. № 3. С. 14-22.

119. Дэн Хуэй. Законодательные варианты административного надзора за защитой личной информации в нашей стране // Право Шанхайского университета транспорта. 2020. № 2. С. 140-152.

120. Жердина С.Ю., Двенадцатова Т.И. Защита персональных данных: первые итоги и перспективы судебных дел // Акционерное общество. 2017. № 11. С. 73-79.

121. Климович Е.В. О сущности понятия «персональные данные» как конфиденциальной информации особой категории // Международные юридические чтения: материалы ежегодной международной научно-практической конференции (14 апреля 2005 г.). Омск, 2005. Ч. 2. С. 21-30.

122. Ковалева Н. Н., Жирнова Н. А. Правовой режим персональных данных в социальных сетях: проблемы квалификации и практические аспекты обработки // Закон. 2025. № 9. С. 61–68.

123. Кротов А.В. Конституционализация права на частную жизнь в решениях органов конституционного правосудия // Журнал зарубежного законодательства и сравнительного правоведения. 2018. № 2. С. 5-14.

124. Кун Сянвэнь. Теоретическая критика и практические размышления о праве на самоопределение персональной информации: применение права принимать решения, предусмотренного статьей 44 Закона КНР о защите персональной информации // Исследование о модернизации системы верховенства права. 2022. № 4. С. 78-97.

125. Кун Фаньхуа. Защита личной конфиденциальности при раскрытии правительственной информации // Исследование административного права. 2020. № 1. С. 17-29.

126. Курлевский И.В. Проблемы защиты персональных данных граждан Российской Федерации в условиях развития информационного общества // Научно-практический электронный журнал Аллея Науки. 2019. №5(32). Alley-science.ru (дата обращения: 30.12.2024).

127. Кучуради И. Понятия человеческого достоинства и прав человека // Вопросы философии. 2018. № 5. С. 43-51.

128. Лапутько К. В. К вопросу о неприкосновенности частной жизни и защите данных // Право.by. 2022. № 1. С. 111-115.

129. Лескина Э.И. Понятие и объект оборота данных // Законодательство. 2025. № 3. С. 42 49.

130. Лескина Э.И., Солдаткина О.Л. Правовое регулирование оборота данных в цифровом виде в Индии: изменения последних лет и тенденции развития // Закон. 2025. № 8. С. 66-76.

131. Ли И. Ценностная дилемма и меры по защите персональных данных: с точки зрения разрешения конфликта между человеческим достоинством и свободой информации // Юридическая наука Хэбэя. 2013. №. 2. С. 2-7.

132. Ли Лей. «Человеческое достоинство» в конституционном праве // Журнал Университета Сунь Ятсена. Общественные наука. 2002. № 6. С. 129-136.

133. Ли Чжунся. Конституционное закрепление прав на неприкосновенность частной жизни в цифровую эпоху // Журнал Восточно-Китайского политико-юридического университета. 2021. № 3. С. 42-54.

134. Ли Япин, Чжоу Вэйлян. Стратегия динамического надзора за защитой личной информации в режиме онлайн // Журнал Чунцинского технологического университета. Общественные науки. 2021. № 11. С. 125-134.

135. Лин Лайфань. Человеческое достоинство и достоинство человеческой личности: обсуждение о методах толкования статьи 38 Конституции КНР // Чжэцзянские общественные науки. 2008. № 3. С. 47-55+126.

136. Линь Лайфань, Ло Чжэнъянь. Права личности в конституции // Юрист. 2008. № 5. С. 60-66.

137. Линь Лайфань, Цзи Яньминь. Значение защиты прав человека в качесвте принципа // Исследование в области права и бизнеса. 2005. № 4. С. 64-69.

138. Линь Лайфань, Чжай Гоцян. О конкуренции между основными правами // Юрист. 2006. № 5. С. 59-66.

139. Лушников А.М. Защита персональных данных работника: сравнительно-правовой комментарий гл.14 Трудового кодекса РФ // Трудовое право. 2009. № 9. С. 93–101.

140. Лю Цзяньлун. О конкуренции между основными правами // Юрист. 2018. № 1. С. 33-49+192-193.

141. Лю Цюань. Различия в позиционировании права на защиту личной информации и их разрешение // Обзор законодательства Китая. 2022. № 6. С. 107-120.

142. Лю Дэлян. Защита прав собственности на персональную информацию // Китайский юридический журнал. 2007. № 3. С. 80-91.

143. Ма Цзин. Защита персональной информации при раскрытии правительством информации: соображения, вызванные услугами запросов по удостоверениям личности Министерства общественной безопасности // Журнал Баодинского института. 2009. № 6. С. 48-50.

144. Майоров А.А. Информационное поле // Славянский форум. 2013. № 2(4). С.144-150.

145. Минбалеев А. В. Проблемы обработки персональных данных журналистами и СМИ // Вестник УрФО. Безопасность в информационной сфере. 2012. № 2(4). С. 26.

146. Минбалеев А. В., Филоненкова В. А. Проблемы защиты персональных данных и цифрового профиля человека в сети Интернет в условиях пандемии // Вестник Южно-Уральского государственного университета. Серия : Право. 2020. Т. 20. № 3. С. 89.

147. Минбалеев А.В. Новеллы законодательства о персональных данных //Университетские правовые диалоги: материалы Международ ной научно-практической конференции, 30–31 марта 2023 г. / под ред. Е.В. Титовой. – Челябинск: Издательский центр ЮУрГУ. 2023. С.108.

148. Минбалеев А.В. Проблемные вопросы понятия и сущности персональных данных // Вестник УрФО. Безопасность в информационной сфере. 2012. № 2 (14). С. 4—9.

149. Минбалеев А.В. Проблемы правового обеспечения кибербезопасности при распространении персональных данных в сети интернет по обновленному законодательству // Вестник УрФО № 2(40). 2021. С. 66.

150. Минбалеев А.В. Трансформация правового режима персональных данных// Устойчивое развитие России: правовое измерение : сборник докладов X Московского юридического форума : в 3 ч. Часть 1. М. : Издательский центр Университета имени О.Е. Кутафина (МГЮА). 2023. С.163.

151. Мираев А.Г. Понятие персональных данных в Российской Федерации и Европейском союзе // Юридическая наука. 2019. №5. С. 76-82.

152. Мусалова З.М. Понятие достоинства личности и эволюция представлений о нем // Юридический вестник ДГУ. 2017. Т. 24. № 4. С. 90-94.

153. Мустафова А.Ю. Защита персональных данных в цифровом пространстве // Барометр экономики, правления и права. 2023. №4 (36). С. 23-27.

154. Мэй Сяин. Юридические атрибуты данных и их гражданско-правовое позиционирование // Китайские общественные науки. 2016. № 9. С. 164-183+209.

155. Наумов В.Б. Задача обеспечения тайны идентификации в информационном праве // Мониторинг правоприменения №3 (32). 2019. С.71.

156. Оботурова Н.С. Концепт достоинства человека и его нравственно-правовое значение // Сетевой научно-практический журнал частного и публичного права. 2022. № 5 (20). С. 27-33.

157. Ожерельева Т.А. Информационное пространство как инструмент поддержки принятия решений // Славянский форум. 2016. № 4 (14). С.169-175.

158. Параскевов А.В., Левченко А.В., Кухоль Ю.А. Сравнительный анализ правового регулирования защиты персональных данных в России и за рубежом // Научный журнал КубГАУ. 2015. № 110 (06). С. 866-894.

159. Петрыкина Н.И. К вопросу о конфиденциальности персональных данных // Законы России: опыт, анализ, практика. 2007. № 6. С. 115-122.

160. Пилипенко С.Г., Федосин С.А. К вопросу о защите права на неприкосновенность частной жизни при обработке персональных данных // Актуальные проблемы современного государства и права: материалы Всероссийской научно-практической конференции (Саранск, 22–23 мая 2008 г.). М. 2009. С. 69-75.

161. Писарев В.В. Обзор развития законодательства США о персональных данных // Вопросы российского и международного права. 2023. Т 13. № 7. С. 95-103.

162. Поликанина О. А., Поликанин А. Н., Шабурова А. В. Организация защиты персональных данных в государственных и муниципальных информационных системах // Интерэкспо Гео-Сибирь. 2022. Т. 6. С. 197-203.

163. Полякова Т.А., Смирнов А.А. Противодействие киберпреступности в новой цифровой реальности: вызовы и правовые решения // Государство и право. 2026. №. 2. С. 236-246.

164. Полякова Т.А., Смирнов А.А. Правовые аспекты обеспечения информационной безопасности при использовании технологий искусственного

интеллекта // Вестник Московского университета. Серия 26: Государственный аудит. 2024. № 3. С. 89-106.

165. Проскурякова М.И. Конституционно-правовые рамки защиты персональных данных в России // Вестник СПбГУ. Сер. 14. Право. 2016. Вып. 2. С. 12-27.

166. Пэн Чжунь. Защита персональной информации с точки зрения Конституции: разъяснение характера, установление интенсивности и координация механизмов // Исследование о модернизации системы верховенства права. 2022. № 4. С. 50-64.

167. Пэн Чэнсинь, Ян Сыи. Атрибуты прав и построения системы в отношении данных, информации и неприкосновенности частной жизни // Журнал Северо-Западного политехнического университета. Общественные науки. 2020. № 2. С. 79-89.

168. Рачицкая В.А. К анализу современных тенденций в сфере защиты данных потребителей // Via scientiarum – Дорога знаний. 2019. № 4. С. 28-31.

169. Савельев А.И. Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) // Право. Журнал Высшей школы экономики. 2015. №1. С. 43–66.

170. Се Либин. Китайско-немецкое сравнение человеческого достоинства в конституции: дискуссия с профессором Линь Лайфанем // Политический и юридический форум. 2010. № 4. С. 53-67.

171. Се Юаньян. Ценность личной информации с точки зрения теории информации: обзор модели защиты прав на неприкосновенность частной жизни // Юридический журнал университета Цинхуа. 2015. № 3. С. 94-110.

172. Се Яовэнь. Защита личной информации в электронном правительстве: опыт США и рекомендации // Административное управление в Китае. 2019. № 2. С. 140-146.

173. Симонова Е.В. Определение понятия персональных данных в Российской Федерации // Молодой ученый. 2017. № 10 (144). С. 323-326.

174. Соколова О.С. Правовые позиции Конституционного Суда Российской Федерации в сфере персональных данных // Современное право. 2015. №10. С. 88-93.

175. Стиглиц, Сун Хуалинь. Свобода, право знать и публичный дискурс: роль прозрачности в общественной жизни // Глобальный юридический обзор. 2002. № 3. С. 263-273.

176. Сычева М. И. Проблемы правового регулирования защиты персональных данных в сети Интернет // Международный журнал гуманитарных и естественных наук. 2022. № 10–3 (73). С. 175.

177. Тан Жуйфан. Законодательная база, нормативное значение и системная структура защиты персональной информации: на основе положения законодательной базы Закона КНР о защите персональной информации // Хунаньские общественные науки. 2022. № 5. С. 109-117.

178. Терещенко Л . К . Государственный контроль в сфере за щиты персональных данных // Право . Журнал Высшей школы экономики . 2018 . № 4 . С . 142–161.

179. Труфанова Е.О. Приватное и публичное в цифровом пространстве: размывание границ // Galactica Media: Journal of Media Studies. 2021. № 1. С. 14-38.

180. У Цянь, Чэнь Яньлин. Правовая защита персональных данных в сфере электронного правительства // Журнал Юго-Западного нефтяного университета. Общественные науки. 2022. № 1. С. 86-96.

181. Фу Синьхуа. Подтверждение права на персональную информацию // Павовая система и социальное развитие. 2021. № 5. С. 123-140.

182. Хан Даюань, Сяо Цзюньфэн. Нормативное действие положения о правах человека в нашей Конституции // Северное право. 2024. № 18(03). С. 6-24.

183. Хан Даюань. Нормативный анализ положения о правах человека в тексте Конституции // Юрист. 2004. № 4. С. 8-13.

184. Химченко, А.И. Формирование цифровой среды доверия: динамика развития инфраструктуры идентификации при реализации цифровых услуг / А.И.

Химченко // Вестник Университета имени О.Е. Кутафина (МГЮА). 2023. № 2. Ч. 101–109

185. Ху Вэньтао. Концепция определения личной чувствительной информации в нашей стране // Юридическая наука в Китае. 2018. № 5. С. 235-254.

186. Хужокова И. Право на неприкосновенность частной жизни в системе прав человека // Сравнительное конституционное обозрение. 2007. № 2. С. 32-36.

187. Хун Данна. Корректировка конституционного значения алгоритмической дискриминации: на основе уважения человеческого достоинства // Политика и право. 2020. № 8. С. 27-37.

188. Хун Данна. Легитимность права забвения в эпоху больших данных // Журнал Южно-Китайского технологического университета. Общественные науки. 2021. № 1. С. 73-83.

189. Хун Данна. Место права на персональную информацию в системе конституционных прав нашей страны// Научный журнал о праве. 2024. № 3. С. 87-105

190. Цадыкова Э.А. Гарантии охраны и защиты персональных данных человека и гражданина // Конституционное и муниципальное право. 2007. № 14. С. 15-19.

191. Цветков В.Я., Рогов А.И., Титов Е.К. Социальная кибернетика в цифровой трансформации общества // ИТ-СТАНДАРТ. 2021. № 1 (26). С. 4-9.

192. Цзи Хайлун. Частноправовое позиционирование и защита данных // Китайский юридический журнал. 2018. № 6. С. 72-91.

193. Цзоу Дуншэн. Раскрытие правительством данных и защита личной конфиденциальности: пример Канады // Административное управление Китая. 2018. № 6. С. 75-82.

194. Цзян Фэн. Скрытые опасения по поводу конституционализации прав: мышление, сосредоточенное на социальных правах // Цинхуаское право. 2010. № 4(05). С. 51-63.

195. Цзян Юнфу, Лю Синь. Об информационной справедливости // Библиотека и информация. 2005. № 6. С. 2-5, 22.

196. Цзян Юнфу, Хуан Лися. Свобода информации, информационные права и публичная библиотечная система // Документы, информация и знания. 2005. № 1. С. 20-23.

197. Ци Айминь. Исследование законодательства о защите персональной информации // Юридическая наука Хэбэя. 2008. № 4. С. 15-33.

198. Цинь Цяньхун, Ди Гаоян. Сорок лет системы проверки конституционности в Китае // Академия. 2019. № 4. С. 47-63.

199. Чернусь, Н. Ю., Чжун, Я. Проблемы правовой защиты персональных данных по законодательству России и Китая. Respublica Literaria. 2024. Т. 5.№ 1. С.113-123.

200. Чехарина В.И. О конституционализации права на защиту персональных данных: из зарубежного опыта // International Journal of Humanities and Natural Sciences. 2020. vol. 3-2 (42). С. 223-228.

201. Чжан Вэйвэй. Положение о правах человека: место нахождения для прав, не перечисленных в Конституции // Юридические обзоры. 2011. № 29(01). С. 10-17.

202. Чжан Синьбао. О структуре прав и интересов в сфере персональной информации // Китайское и иностранное право. 2021. № 5. С. 1144-1166.

203. Чжан Синьбао. От конфиденциальности к личной информации: теория и институциональные механизмы повторного измерения интересов // Юридическая наука в Китае. 2015. № 3. С. 38-59.

204. Чжан Сян. Двойственная природа основных прав // Китайский юридический журнал. 2005. № 3. С. 21-36.

205. Чжан Сян. Категория человеческого достоинства в Конституции: на основе защиты личностного права в ГК и персональной информации // Юридические обзоры в Китае. 2023. № 1. С. 57-67.

206. Чжан Сян. Конституционное подтверждение права на персональную информацию на основе размышления о теории разделения защиты и теории доминирования // Глобальный юридический обзор. 2022. № 1. С. 53-68.

207. Чжан Сян. Конституционное толкование права на переписку и рамки проверки: обсуждение с Ду Цянцяном, Ван Каем и Цинь Сяоцзянем // Журнал сравнительного правоведения. 2021. № 1. С. 33-48.

208. Чжан Янь, Сюй Цзясинь. Переосмысление права на корреспонденцию в цифровую эпоху // Журнал «Чи-Лу». 2022. № 5. С. 94-105.

209. Чжао Хун. Обязательство государства защищать право на персональную информацию в контексте нового Гражданского кодекса // Обзор экономического и торгового права. 2021. № 2. С. 1-20.

210. Чжао Хун. Текущая ситуация с защитой права на информационное самоопределение в нашей стране и перспективы развития законодательства в этой области // Обзор законодательства Китая. 2017. № 1. С. 147-161.

211. Чжоу Вэйдун. Конституционная систематизация прав на персональные данные // Правоведение. 2023. № 1. С. 32-48.

212. Чжоу Ханьхуа. Изучение способа совместимого управления персональными данными - законодательное направление Закона Китая о защите личной информации // Китайский юридический журнал. 2018. № 2. С. 3-23

213. Чжоу Ханьхуа. Правовое позиционирование защиты личной информации // Исследования в области права и бизнеса. 2020. № 3. С. 44-56.

214. Чжоу Ююн. Духовный темперамент основного административного кодекса Китая // Политический и юридический форум. 2022. № 40(03). С. 61-77.

215. Чжу Чжэнь. Модель защиты прав: общественный характер и права в области защиты личной информации // Глобальный юридический обзор. 2022. № 1. С. 21-35.

216. Чжэн Гэ. Закон алгоритмов и алгоритм законов // Обзор законодательства Китая. 2018. № 2. С. 66-85.

217. Чубукова С.Г. Правовые проблемы защиты генетической информации: субъектный подход // Вестник университета имени О.Е. Кутафина. 2020. №.5. С. 102.

218. Чэн Сяо. О правах на персональные данные в эпоху больших данных // Китайские общественные науки. 2018. № 3. С. 102-122.

219. Чэнь Кэсян. Основы реализации и институциональная логика административных наказаний в области защиты личной информации // Юридическая наука. 2023. № 11. С. 57-72.

220. Чэнь Танфа. Обсуждение дилеммы и правил защиты конфиденциальности в Интернете и среде больших данных // Цзинаньский Журнал. Философия и общественные науки. 2015. № 10. С. 126-130.

221. Шень Вэйсин. Реконструкция системы цифровых прав: на пути к дифференцированному подходу к неприкосновенности частной жизни, информации и данным // Политический и юридический форум (Журнал Китайского политико-юридического университета). 2022. № 3. С. 89-102.

222. Ши Цзяю. Частноправовой аспект защиты личной информации: обсуждение взаимосвязи между Гражданским кодексом и Законом о защите персональной информации // Журнал сравнительного правоведения. 2021. № 5. С. 14-32.

223. Ши Яньцзюнь. Реальная дилемма открытого использования государственных данных в эпоху больших данных и пути к его правовому обеспечению // Журнал Пекинского университета почты и телекоммуникаций. Общественные науки. 2023. № 6. С. 70-78.

224. Шэнь Ян, Лю Гохуа. Административно-правовая защита персональных данных граждан в контексте больших данных // Внешняя торговля и экономика. 2020. № 5. С. 111-116.

225. Юань Дуньлян. Уголовно-правовая защита личной информации при использовании технологии cookie // Журнал западных исследований. 2021. № 22. С. 56-58.

226. Ян Фан. Теория права на самоопределение персональной информации и ее просмотр и объект защиты Закона КНР о защите персональной информации // Журнал сравнительного правоведения. 2015. № 6. С. 22-33.

227. Янь Цуньшэн. Исследование легитимности закона // Юридическая наука (Журнал Северо-Западного политико-юридического университета. 2002. № 3. С. 3-14.

228. Яо Юэжун. Подтверждение права на информационное самоопределение как одно из основных прав в нашей стране // Политика и право. 2012. № 4. С. 72-83.

**2.3. Литература на английском языке**

229. Beigner, B. La protection de la vie privee / B. Beigner // Libertes et Droits fondamentaux. – Paris: Dalloz, 2003. P. 161–163.

230. Defilippis A.J. Securing Information Ships: Recognizing a Right to Privity in Fourth Amendment Jurisprudence[J]. The Yale Law Journal, 2006,115(5): 1086-1121.

231. Hardy K., & Maurushat A. Opening up Government Data for Big Data Analysis and Public Benefit[J]. Computer Law & Security Review, 2017,33(1): 33-37.

232. Post R.C, & Rothman J.E. The First Amendment and the Right(s) of Publicity[J]. Yale Law Journal, 2020,130(1): 86-172.

233. Schwartz P.M., & Solove D.J. The PII Problem: Privacy and a New Concept of Personally Identifiable Information[J]. New York University Law Review, 2011,86(6): 1814-1894.

234. Strahilevitz, L.J. Reunifying Privacy Law[J]. California Law Review, 2010,98(6): 2007-2048.

235. Thomas F. Smedingoff, Online law, 1996: 269-270.

236. Tsvetkov V. Ya. Information Space, Information Field, Information Environment // European researcher. 2014. № 8-1 (80):1416-1422

237. Veil W. The GDPR: The Emperor’s New Clothes-On the Structural Shortcomings of Both the Old and the New Data Protection Law[J]. Neue Zeitschrift für Verwaltungsrecht, 2018, 10(2018): 686.

238. Waldman A.E. Privacy as Trust: Sharing Personal Information in a Networked World[J]. University of Miami Law Review, 2015,69(3): 559-630.

**2.4. Диссертации, авторефераты диссертаций**

239. Белгородцева Н.Г. Теоретико-правовые аспекты защиты персональных данных: автореф. дис. ... канд. юрид. наук: 12.00.01. М., 2012. 25 с.

240. Бундин М.В. Персональные данные в системе информации ограниченного доступа: дисс… канд. юрид. наук. М., 2017. 218 с.

241. Ван Цици. Исследование правовых основ и институционального построения открытости государственных данных: дисс. … докт. юрид. наук / Ван Цици. – Пекин: Национальная академия управления. 2022. 190 с.

242. Вельдер И.А. Система правовой защиты персональных данных в Европейском союзе: дис. ... канд. юрид. наук: 12.00.10. Казань, 2006. 165 с.

243. Го Сюаньцзы. Исследование по защите конфиденциальности при трансграничной передаче персональных данных: дисс. … докт. юрид. наук / Го Сюаньцзы. – Чанчунь: Цзилиньский университет. 2024. 148 с.

244. Кучеренко А.В. Правовое регулирование персональных данных в Российской Федерации: автореф. дис. … канд. юрид. наук. Челябинск, 2010. 23 с.

245. Ни Цяньмяо. Исследование системы правовой защиты прав собственности на данные: дисс. … докт. юрид. наук / Ни Цяньмяо. – Чунцин: Юго-Западный политико-юридический университет. 2023. 242 с.

246. Федосин А.С. Защита конституционного права человека и гражданина на неприкосновенность частной жизни при автоматизированной обработке персональных данных в Российской Федерации: автореф. дис. канд. юрид. наук: 12.00.14. Саранск, 2009. 27 с.

247. Хужокова И. М. Конституционное право человека и гражданина на неприкосновенность частной жизни в Российской Федерации: автореф. дис. … канд. юрид. наук. Саратов, 2007. 26 с.

248. Юань Цюань. Исследование системы классификационной защиты персональной информации в контексте больших данных: дисс. … докт. юрид. наук / Юань Цюань. – Пекин: Университет международного бизнеса и экономики, 2019. 171 с.

# ПРИЛОЖЕНИЯ

Приложение 1

Таблица. Типы персональных данных и их состав[424]

| | Типы | Состав | Степень чувствительности |
|---|---|---|---|
| 1 | Сведения о личности | информация о удостоверении личности, паспорте, водительских правах и т.д. | +++++ |
| 2 | Биометрическая информация | Отпечатки пальцев, отпечатки голоса, данные для распознавания лиц и т.д. | +++++ |
| 3 | информация о спорте и состоянии здоровья | Сведения медицинского характера и информация о здоровье, такая как рост, вес, объем легких и т.д. | +++++ |
| 4 | Информация Об интимной жизни и предпочтениях | Интимная жизнь, политические взгляды, религиозные убеждения, предвыборные предпочтения | +++++ |
| 5 | Информация о личной собственности | Идентификационная информация, Банковский счет, информация о депозите, виртуальные транзакции и т.д. | +++++ |
| 6 | Информация о личном местоположении | Информация о местоположении в режиме реального времени и т.д. | +++ |
| 7 | Базовые личные данные | ф.и., дата рождения, пол, адрес, личный номер телефона и т.д. | +++ |
| 8 | Коммуникационные данные | Записи о переписке, SMS, электронная почта и т.д. | +++ |
| 9 | Цифровой след | Запись действий пользователя, включая записи о просмотре веб-сайтов, кликах и т.д. | +++ |
| 1 | Контактные | Адресная книга, запись друзей, список | +++ |

[424] Согласно типологии, формируемой в Китае. См.: Ху Вэньтао Концепция определения личной чувствительной информации в нашей стране // Юридическая наука в Китае. 2018. № 5. 235-254.

| | | | |
|---|---|---|---|
| 0 | данные | адресов электронной почты и т.д. | |
| 11 | Информация об устройстве | серийный номер оборудования, уникальный идентификационный код оборудования и т.д. | ++ |
| 12 | Сетевая идентификационная информация | учетная запись (аккаунт), IP-адрес | ++ |
| 13 | Информация о личном использовании | пользовательский контент и т.д. | ++ |

Примечания: «+» указывает на единицу измерения чувствительности.

Приложение 2

Таблица. Сходства и различия между Законом РФ о ПДн и Законом КНР о ПДн

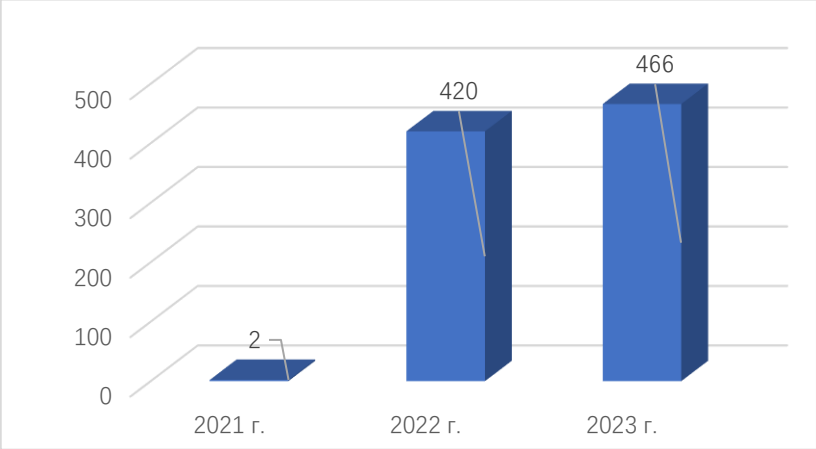
| | Россия | Китай |
|---|---|---|
| Законодательство | Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ | Закон КНР о защите персональной информации от 01.11.2021 г. |
| Классификация персональныхданных | 4 категории:<br>персональные данные общего режима;<br>общедоступные;<br>биометрические;<br>специальные категории персональных данных | 2 категории:<br>чувствительные и обычные |
| Принципы | Законность и справедливость;<br>соответствие цели;<br>точность, достаточность и актуальность;<br>необходимость и добросовестность. Отдельно выделен принцип обеспечения конфиденциальности | Законности, правомерности, необходимости и добросовестности;<br>ограничения цели;<br>открытости и прозрачности;<br>целостности и правильности;<br>обеспечения безопасности |
| Согласие | Требуется перед сбором персональных данных | Требуется перед сбором персональных данных |
| Меры безопасности | Должны быть приняты для защиты личных данных | Должны быть приняты для защиты личных данных |
| Права физических лиц | Право на доступ и исправление личных данных | Всеобъемлющие права, включая право<br>на доступ, исправление, удаление и передачу личных данных |
| Хранилище данных | Должны храниться на территории Российской Федерации | Нет такого требования |
| Отчет об утечке данных | Установлены процедуры уведомления<br>уполномоченного органа | Должен сообщить об утечке данных в уполномоченный орган и заинтересованным лицам |

| | | |
|---|---|---|
| Специальные положения об обработке персональных данных государственными органами | Не имеется отдельный раздел в законе персональных данных | Имеется отдельный отдел в законе о персональных данных |
| Трансграничная передача | Специальные правила трансграничного предоставления персональных данных | Специальные правила трансграничного предоставления персональных данных |
| Уполномоченный орган по защите персональных данных | Роскомнадзор. Отдельные полномочия у ФСБ, ФСТЭК | Государственная администрация по киберпространству; отделы при Госсовете |

Приложение 3

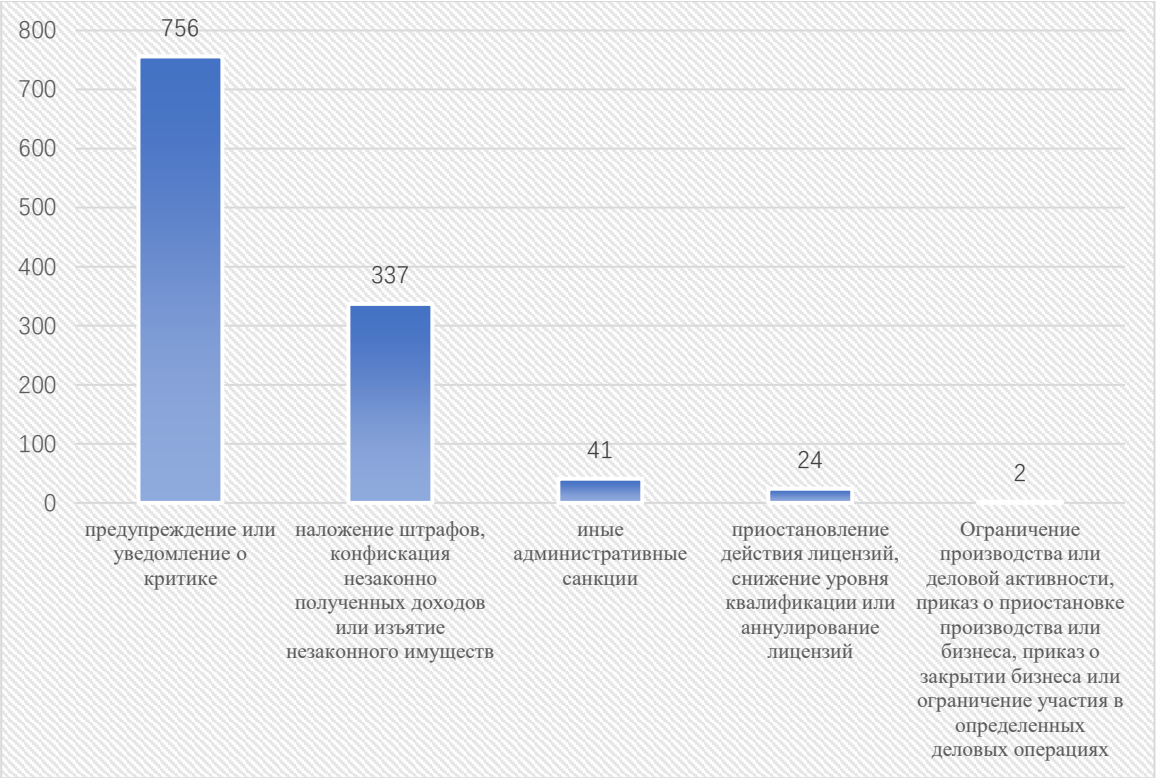
Диаграмма. Количество дел об административных правонарушениях в отношении персональных данных в Китае

(за 2021-2023 годы)



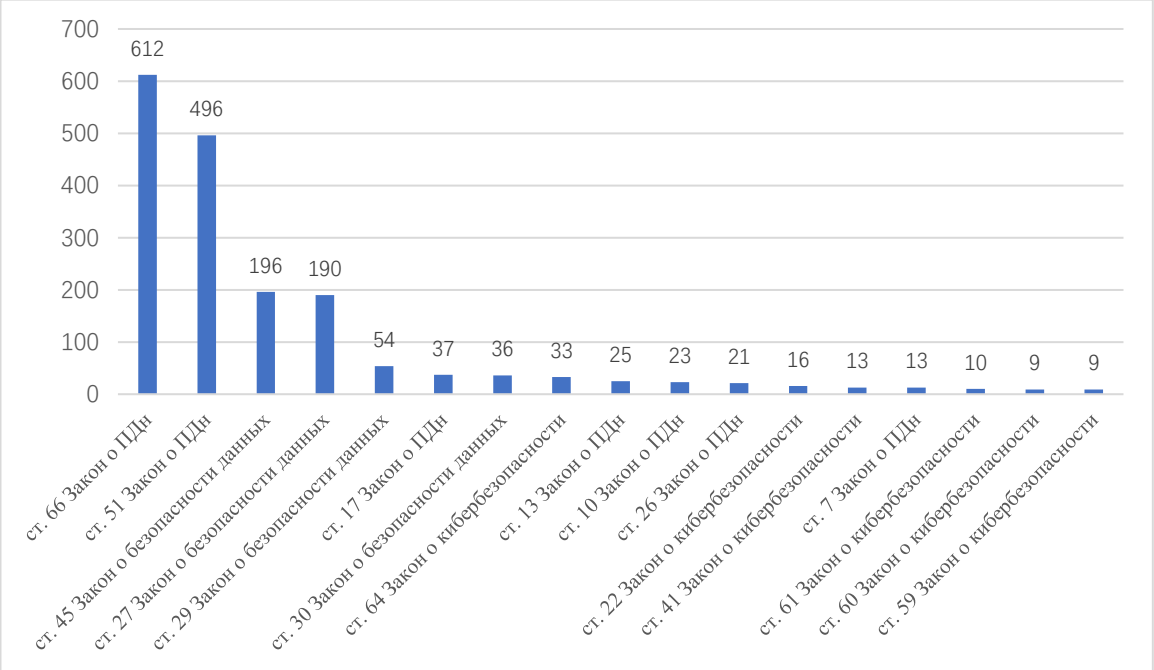
Приложение 4

Диаграмма. Виды административных наказаний, применимых в сфере персональных данных в Китае



Приложение 5

Диаграмма. Количество выявленных административных правонарушений в сфере персональных данных в Китае по отдельным составам



Приложение 6

Диаграмма. Утечки персональных данных в различных отраслях Китая в 2024 году

