УДК 34.096 DOI: 10.31249/iajpravo/2026.01.12

ГЛОТОВ С.А.[1] «ЦИФРОВОЙ КИТАЙ»: ОБЗОР ЗАКОНОДАТЕЛЬНЫХ АКТОВ КИТАЙСКОЙ НАРОДНОЙ РЕСПУБЛИКИ, РЕГУЛИРУЮЩИХ ВОПРОСЫ КИБЕРБЕЗОПАСНОСТИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Аннотация. В обзоре рассматриваются три ключевых акта Китайской Народной Республики, регулирующих отношения в области цифровизции, больших данных, цифровой экономики. Это Закон о кибербезопасности КНР; Закон о безопасности данных КНР; Закон о защите персональных данных КНР.

Ключевые слова: Китай; цифровизация; цифровое право; кибербезопасность; защита данных; утечка данных; безопасность данных; персональные данные; объекты критической инфраструктуры; мониторинг безопасности данных; юридическая ответственность.

GLOTOV S.A. “Digital China”: review of legislative acts of the people's republic of china regulating cybersecurity and personal data protection

Abstract. The review examines three key acts of the People's Republic of China regulating relations in the field of digitalization, big data, and the digital economy. These are the Cybersecurity Law of the People's Republic of China; the Data Security Law of the People's Republic of China; the Law on the Protection of Personal Data of the People's Republic of China.

Keywords: China; digitalization; digital law; cybersecurity; data protection; data leakage; data security; personal data; critical infrastructure facilities; data security monitoring; legal responsibility.

[1] *Глотов Сергей Александрович*, ведущий научный сотрудник отдела правоведения ИНИОН РАН, доктор юридических наук, профессор.

Для цитирования: Глотов С.А. «Цифровой Китай»: Обзор законодательных актов КНР, регулирующих вопросы кибербезопасности и защиты персональных данных // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4: Государство и право. – 2026. – № 1. – С. 182–198. – DOI: 10.31249/iajpravo/2026.01.12

Введение

В 2025 г. в издательстве «Проспект» вышла книга «Избранные нормативно-правовые акты Китайской Народной Республики в области цифровизации»[1], которая содержит тексты законов КНР, регулирующие отношения в сферах кибербезопасности и защиты данных, в том числе персональных. Данный сборник избранных нормативных правовых актов КНР для российского читателя, прежде всего юристов, перевела Ли Яо, доктор юридических наук из Института верховенства права за рубежом при Восточно-Китайском университете политических наук и права.

В предисловии к этому сборнику Ли Яо замечает, что «искусственный интеллект создает много удобного и эффективного для жизни общества, однако и порождает потенциальные сокрушительные риски, которые в основном отражаются в ряде вопросов, таких как защита конфиденциальности, дискриминация данных, трансграничные данные, безопасность данных и др. (…) Юристам всего мира необходимо активно реагировать на них и добиваться баланса между безопасностью данных и экономическим развитием, выстраивая правовую систему, обеспечивающую национальную безопасность, общественные интересы, защиту законных прав граждан и юридических лиц и других организаций в киберпространстве» (с. 3).

КНР стала одной из ведущих стран мира в развитии цифровой экономики, больших данных и искусственного интеллекта, машинного обучения, мобильных платежей блокчейна, умного правосудия и т.д. Ли Яо приводит такие данные: в 2023 г. объем цифровой экономики Китая достиг 53,9 трлн юаней, доля цифровой экономики в ВВП КНР составляет 42,8% (там же). Это подтверждается и показателями, уже 2024–2025 гг., а также тем, что Китай является сегодня общепризнанной мировой фабрикой това-

[1] См.: Избранные нормативно-правовые акты Китайской Народной Республики в области цифровизации / пер. с кит. Ли Яо. – Москва: Проспект, 2025. – 136 с.

ров, да и во многом услуг. С помощью «цифры» и других инструментов ведения бизнеса и администрирования ему удалось стать второй экономикой мира.

Достигнуть подобного рода результатов невозможно без качественного эффективного правового обеспечения, и в этой связи китайский опыт правового регулирования в области цифровизации, кибербезопасности, защиты данных интересен и для российской научной общественности.

В сборник законов КНР в рассматриваемой области включены не только законы КНР в сфере цифровизации, принятые Всекитайским собранием народных представителей (ВСНП), но и различные положения, утвержденные постановлениями Государственного совета КНР с указанием их срока вступления в силу (например постановление Госсовета КНР № 745 «О защите безопасности критической информационной инфраструктуры» от 27.04.2021 г., вступившее в силу с 01.09.2021 г.).

В данном обзоре кратко анализируются основные положения следующих законов КНР в области цифровизации.

№ п/п.	Наименование законов, включенных в сборник, и количество статей в них	Время принятия Постоянным комитетом ВСНП и вступления их в силу
1	Закон о кибербезопасности КНР, содержит 79 статей	Принят 07.11.2016 г. Вступил в силу 01.01.2017 г.
2.	Закон о безопасности данных КНР – 55 статей	Принят 10.06.2021 г. Вступил в силу 01.09.2021 г.
~~3~~	Закон о защите персональных данных КНР – 74 статьи	Принят 20.08.2021 г. Вступил в силу 01.11.2021 г.

Закон КНР о кибербезопасности

Закон о кибербезопасности принят в целях «поддержания суверенного киберпространства и национальной безопасности, социальных общественных интересов, защиты законных прав и интересов граждан, юридических лиц и других организаций, а также содействия здоровому развитию информатизации экономики и общества» (ст. 1).

Следует отметить, что понятие «кибербезопасность» определяется в ст. 76 Закона гл. 7 «Дополнительные положения». В ней *Кибербезопасность* понимается как «способность предотвращать атаки, вторжение, вмешательство, разрушение и незаконное использование сети, а также аварии, путем принятия необходимых мер для поддержания сети в стабильном и надежном состоянии, а

также для обеспечения целостности, конфиденциальности и доступной сети».

Указанная статья определяет: «*сеть* – это система, состоящая из компонентов или других информационных терминалов и соответствующего оборудования, которая собирает, хранит, передает, обменивается и обрабатывает информацию, согласно с определенными правилами и процедурами»; «*операторы сетей* – владельцы и администраторы сетей и поставщики сетевых услуг; сетевые данные – все виды электронных данных, собираемых, хранимых, передаваемых, обрабатываемых и создаваемых в сети»; «*персональные данные* – все виды информации, записанные в электронном или ином виде, которая может идентифицировать личность физического лица, отдельно или в сочетании с другой информацией, включая, но не ограничиваясь ФИО физического лица, дату рождения, номер документа, удостоверяющего личность, личную биометрическую информацию, адрес проживания, номер телефона и т.д.».

Структура Закона КНР о кибербезопасности: общие положения (гл. 1); вопросы поддержания кибербезопасности и продвижения ее на государственном уровне (гл. 2); правовой режим безопасности сетевых операций (гл. 3); безопасность самих сетей (гл. 4); а также создание системы мониторинга и раннего предупреждения кибербезопасности (гл. 5) и юридической ответственности (гл. 6), дополнительные положения (гл. 7).

Закон устанавливает:

1. *Права и обязанности государства в сфере кибербезопасности*. Государство формирует и постоянно совершенствует стратегию кибербезопасности, определяет основные требования и главные цели по обеспечению кибербезопасности, предлагает политику, задачи и меры по обеспечению кибербезопасности в ключевых отраслях (ст. 4). Государство: выявляет угрозы кибербезопасности, определяет и реализует меры по поддержанию безопасности и порядка в киберпространстве (ст. 5), «пропагандирует честное добросовестное полезное и цивилизованное поведение в интернете» (ст. 6); активно участвует в международных обменах и сотрудничестве в области управления киберпространством (ст. 7).

Государственный департамент сетевой информации, отвечающий за координацию работы по обеспечению кибербезопасности (ст. 8), участвует в создании и эксплуатации сетей Интернет, улучшает уровень веб-сервисов, обеспечивает их безопасность (ст. 10, 12); защищает права граждан и юридических лиц, органи-

заций, работающих в сети (ст. 12); поддерживает исследования и разработку сетевых продуктов, способствующих здоровому развитию несовершеннолетних, и наказывает тех, кто использует Интернет, угрожая физическому и психологическому здоровью несовершеннолетних (ст. 13).

За защиту, надзор и управление кибербезопасностью в рамках своих обязанностей отвечает Департамент телекоммуникаций при Государственном совете КНР, Департамент общественной безопасности и другие компетентные органы (ст. 8). В приведенных выше положениях Закона есть важное указание законодателя на конкретные государственные органы, отвечающие за выполнение конкретных норм Закона.

2. *Права и обязанности лиц и организаций в сети Интернет*. Они обязаны: соблюдать Конституцию КНР и законы, общественный порядок и общественную мораль в данной сфере, не должны ставить под угрозу кибербезопасность (ст. 12).

Лица и организации имеют право: сообщать в департамент сетевой информации, телекоммуникации и общественной безопасности о любых действиях, которые ставят под угрозу кибербезопасность (ст. 14); в свою очередь, соответствующие ведомства должны сохранять конфиденциальную информацию, поступившую от осведомителей, и защищать законные права и интересы осведомителей (ст. 14).

3. *Продвижение Концепции и конкретных требований кибербезопасности государством и обществом* (ст. 15–20). Государство создает стандарты кибербезопасности, в том числе отраслевые, связанные как с управлением процессами в данной области, так и с обеспечением безопасности сетевых продуктов и услуг. Эта функция возложена на Административный департамент по стандартизации при Государственном совете, а также госсоветы и народные правительства провинций, автономных районов, городов и т.д. Эта деятельность осуществляется на плановой основе, путем роста инвестиций, поддержки научных исследований и защищает при этом интеллектуальную собственность на сетевые технологии.

Активными проводниками государственной политики кибербезопасности являются предприятия и организации, различные НИИ, вузы и профтехучилища. «Средства массовой информации

проводят массовую пропаганду и просвещение общества по вопросам кибербезопасности» (ст. 19)[1].

4. *Обязанности операторов сетей и безопасность закреплены в ст. 21–50.* Операторы сетей «обязаны защитить сеть от вмешательства, разрушения или несанкционированного доступа, также предотвращать утечку, кражу сетевых данных или фальсификацию (ст. 21). Для этого сетевые операторы предпринимают организационные и технические меры, обеспечивают сохранение соответствующих сетевых данных в течение не менее шести месяцев, их классификацию, разрешение копирования и шифрование наиболее важных данных.

Закон КНР о кибербезопасности также определяет, что *операторы крупнейших инфраструктур* обязаны проверять свои сети не реже одного раза в год в режиме тестирования и оценки, информируя об этом власти, в том числе Государственный департамент сетевой информации. Обращается внимание на то, что операторы сети «должны сохранять строгую конфиденциальность сообщений или информацию о пользователях и создавать надежную систему защиты информации о пользователях (ст. 40), не должны раскрывать, подделывать или уничтожать собранные или персональные данные, не должны предоставлять персональные данные другим лицам без согласия лица, у которого они собраны» (ст. 42), а если «физическое лицо ощущает, что операторы сетей собирают или используют его персональные данные в нарушение положений законов … то операторы сетей обязаны принять меры по удалению или неиспользованию» (ст. 42).

Поставщики сетевых продуктов и услуг не должны устанавливать вредоносные программы; наоборот, обязаны обеспечивать обслуживание безопасности своих продуктов и услуг на постоянной основе, сообщать пользователю и получать согласие на сбор персональных данных, осуществлять сертификацию своих процессов и оборудования, проверять подлинность идентификационной информации, регистрировать доменные имена, своевременно устранять риски безопасности, такие как компьютерные вирусы, сетевые атаки и вторжение в сеть и т.д. (ст. 22–26).

[1] Подробнее об этом см.: Галяшина Е.И., Анонян Е.А., Богатырёв Е.Н. Защита от злоупотребления искусственным интеллектом и нейротехнологиями в аспекте медиабезопасности: монография / отв. ред. Е.И. Галяшина. – Москва: Проспект, 2025. – 272 с.

Закон КНР о кибербезопасности предусматривает, что «ни одно физическое лицо или организация не должны заниматься деятельностью, угрожающей кибербезопасности путем незаконного вторжения в чужие сети, нарушения нормального функционирования чужих сетей, кражи сетевых данных и т.д. (ст. 27)[1]. Важно и то, что «любое лицо или организация несут ответственность за использование сети и не должны создавать веб-сайты или коммуникационные группы с целью совершения мошенничества, обучения преступным методам, изготовления или продажи запрещенных или контролируемых предметов» (ст. 46 Закона) что сегодня становится особенно актуальным.

5. *Мониторинг и раннее предупреждение кибербезопасности, а также вопросы юридической ответственности* (ст. 51–75). Мониторингом раннего предупреждения занимаются отраслевые департаменты, ответственные за защиту безопасности критической инфраструктуры при руководящей (контролирующей) роли государственного департамента сетевой информации.

Закон КНР о кибербезопасности в гл. 6 устанавливает юридическую ответственность операторов, не выполняющих обязательства по защите кибербезопасности: значительные штрафы накладываются как на саму компанию, так и на ее контролирующий и непосредственно отвечающий за работу операторов лиц; возможно приостановление соответствующей деятельности, закрытие веб-сайта, отзыв лицензии и др.(ст. 62).

Согласно ст. 64, к оператору сетей, посягающему на право персональных данных, наряду с уже указанными мерами воздействия могут быть применены и такие, как «конфискация незаконных доходов или штраф в размере не менее двойной и не более десятикратной суммы незаконных доходов», а если незаконных доходов нет, то накладывается штраф в размере не более 1 млн юаней.

Если сетевые операторы хранят информацию из разряда критической информационной инфраструктуры (о чем подробно говорится в ст. 31–39 Закона) за пределами страны или предоставляют данные за пределы страны, в нарушение ст. 37 Закона[2], то их

[1] Об этико-правовой проблематике по данному вопросу см., напр.: Бахтеев Д.В. Искусственный интеллект: этико-правовые основы: монография. – Москва: Проспект, 2025.–176 с.

[2] В ст. 37 Закона КНР о кибербезопасности устанавливается, что персональные данные и важные данные, собранные и созданные операторами, должны храниться на территории страны. Если возникает деловая потребность в передаче

также ожидает предписание об исправлении и предупреждение; конфискация незаконного дохода, штраф в размере не менее 50 тыс. и не более 500 тыс. юаней; приостановка деятельности; закрытие веб-сайта; отзыв лицензии, а также штраф на контролирующий персонал и персонал, непосредственно отвечающий за работу, в размере не менее 10 тыс. и не более 100 тыс. юаней (ст. 66).

Закон КНР о кибербезопасности в ст. 31 содержит перечень критических отраслей критической инфраструктуры, нуждающейся (защищаемой) кибербезопасностью. Это: государственные коммуникации и информационные услуги; энергетика, транспорт, водоснабжение; финансы, государственные услуги; электронное правительство и др.

Критерием важности защиты подобного рода инфраструктуры является факт «повреждения, потери функции или утечки данных», которые «могут серьезно угрожать национальной безопасности, жизнеобеспечению населения и общественным интересам» (ст. 31).

Конкретные рамки «критических информационных структур и мер их защит» определяет Государственный совет КНР.

Указанный Закон в ст. 67 предусматривает возможность карать и тех, кто «создает веб-сайты или коммуникационные группы с целью совершения незаконной деятельности или использует интернет для публикации информации, связанной с совершением незаконной или преступной деятельности».

Если это преступление не влечет уголовной ответственности, то лицам, вставшим на этот путь, грозит: арест на срок не более пяти суток и штраф в размере не менее 10 тыс. и не более 100 тыс. юаней, при отягчающих обстоятельствах арест на срок не менее пяти, но не более 15 суток и штраф в размере не менее 50 тыс. и не более 500 тыс. юаней, а также закрытие веб-сайта и коммуникативной группы.

Приговор по таким делам выносит орган общественной безопасности. Если это касается деятельности не лица, а организации в аналогичных случаях, то на организацию, ее руководящий и контролирующий состав накладывается штраф в размере не менее 100 тыс. и не более 500 тыс. юаней. Приговор также выносит орган общественной безопасности.

этих данных за рубеж, оценки их безопасности и возможности передачи производятся государственным департаментом сетевой информации совместно с соответствующим департаментом Государственного совета КНР.

В ст. 69 Закона КНР о кибербезопасности содержится исчерпывающий перечень действий, за которые операторы несут ответственность, если они не вносят исправления, предписанные соответствующим государственным органом, действующим в сфере обеспечения кибербезопасности: 1) невыполнение требований по уничтожению или удалению запрещенной к публикации, распространению информации; 2) отказ или воспрепятствование осуществлению компетентным департаментом законного надзора и проверок; 3) неоказание технической поддержки и помощи органам общественной и государственной безопасности.

Анализируемый Закон в ст. 73 предусматривает ответственность государственных структур, действующих в сфере безопасности, за пренебрежение их сотрудников своими обязанностями; злоупотребление своими полномочиями; недобросовестную деятельность в целях личной выгоды, если это не является преступлением[1]. Если же в их действиях содержится состав преступления, виновные несут уголовную ответственность в соответствии с законом (ст. 74).

Следует заметить, что некоторые важные положения Закона КНР о кибербезопасности регулируются Гражданским кодексом КНР, принятым в 2020 г., вступившим в силу с 1 января 2021 г. Глава 6 «Право на неприкосновенность частной жизни и защиты персональных данных» ГК КНР (ст. 1032–1039) определяет понятия и содержание права на неприкосновенность частной жизни и персональных данных, условия обработки и ответственности операторов персональных данных, сохранение тайны сведений о личности и ее персональных данных. Статья 1039 ГК КНР устанавливает обязанность органов государственной власти, организаций, наделенных административными функциями, а также их сотрудников сохранять в тайне сведения, относящиеся к личной жизни граждан и их персональным данным, которые становятся им известны в связи с исполнением обязанностей, не вправе распространять указанные сведения и персональные данные или осуществлять их передачу в нарушение закона.

[1] Об уголовной ответственности в Китае см. подробнее: Гео Минсюань. Зарождение, становление и развитие современного уголовного законодательства в Китайской Народной Республике: монография / под науч. ред. Н.А. Сидоровой, И.В. Васильева. – Москва: Проспект, 2025. – 568 с.

Китай: безопасность больших данных

Закон КНР о безопасности данных принят Постоянным комитетом ВСНП спустя пять лет после вступления в силу Закона КНР о кибербезопасности, т.е. в 2021 г. Он содержит семь глав, 55 статей и имеет целью регулировать деятельность информационных властей КНР по отношению безопасности данных, воздействию, развитию и использованию данных законных прав и интересов физических лиц и организаций. Речь идет также о защите национального суверенитета, безопасности и интересов развития Китая и его граждан (ст. 1 Закона о безопасности данных).

Этот Закон регулирует обработку данных как на территории КНР, так и за его пределами. Если это угрожает национальной безопасности Китая, общественным интересам или законным интересам граждан, то речь идет в первую очередь о защите правительственных данных, а также содержит следующие определения понятий, важных для реализации этого Закона.

Данные – любая запись информации с помощью электронных или иных средств обработка данных, включая сбор, хранение, использование, обработку, передачу, предоставление, распространение данных и т.д. (ст. 3).

Безопасность данных – способность гарантировать, что данные находятся в состоянии эффективной защиты и законного использования, а также способность гарантировать постоянное состояние безопасности принимаемых необходимых мер (ст. 3).

Система обеспечения безопасности данных в КНР включает Центральное агентство по руководству национальной безопасностью, отвечающее за безопасность данных национального характера, их изучение, формулирование, выработку «национальной стратегии безопасности данных и соответствующих основных политик, координацию основных вопросов и важных работ по обеспечению национальной безопасности данных» (ст. 5).

Народные правительства на уровне провинций и выше, – согласно ст. 14 Закона, – должны включать развитие цифровой экономики в национальный план экономического и социального развития на местном уровне и разработать план развития цифровой экономики в соответствии с потребностями.

Государство берет на себя целый ряд обязанностей: защиту прав и интересов физических лиц[1] и организаций, связанных с данными; разумное и эффективное использование данных в соответствии с законом, гарантии свободного потока данных в упорядоченном порядке; развитие цифровой экономики, ключевым элементом которой являются данные (ст. 7); пропаганду и распространение знаний о безопасности данных, повышение осведомленности среди населения и уровня защиты данных в обществе, отраслевых организациях, НИИ, на предприятиях и у частных лиц (ст. 9); осуществление международного обмена и сотрудничество в области управления безопасностью данных эксплуатации и использования данных, развитие международных правил и стандартов, связанных с безопасностью данных; обеспечение безопасного и свободного трансграничного потока данных (ст. 12); координацию развития и безопасности, продвижение безопасности данных в промышленном развитии (ст. 13); развитие использования данных для повышения интеллектуального уровня государственных услуг (ст. 15); поддержку исследований в обществе технологий эксплуатации и использование данных и безопасности данных, продвижение технологий и коммерческих инноваций в области данных, в том числе в промышленных разработках и системах (ст. 17); поддержку развития тестирования, оценки, сертификации и других услуг в области безопасности данных (ст. 18); совершенствование системы управления операциями с данными, развитие рынка операций с данными (ст. 19); поддержку образовательных учреждений, НИИ, предприятий в проведении обучения и подготовки кадров, связанных с технологией эксплуатации и использования данных безопасности данных (ст. 20).

Закон КНР о безопасности данных в гл. 3 закрепляет права и обязанности государства в сфере защиты данных. Государство берет на себя следующие обязанности: создание системы классификации и иерархии по защите данных для предотвращения их фальсификации, уничтожения, утечки, незаконного приобретения и использования в области национальной безопасности, жизнеобеспечения национальной экономики, значимых национальных интересов и нужд народа (ст. 21); формирование национального координационного механизма по безопасности данных (ст. 21); совершенствование централизованного единого эффективного и

[1] См., напр.: Ван Лимин. Личные права: учебник. – Москва: Проспект, 2023. – гл. 14: Право на персональные данные. – С. 283–296.

авторитетного механизма оценки рисков безопасности данных отчетности, обмена информацией, мониторинга и раннего предупреждения (ст. 22); создание механизма реагирования на чрезвычайные ситуации, связанные с безопасностью данных, предотвращением расширения ущерба, устранением потенциальных рисков безопасности и своевременного распространения информации о предупреждении общественности, отвечает за это соответствующий компетентный департамент (ст. 23); установление системы проверки безопасности данных; осуществление экспертного контроля в отношении данных, которые также затрагивают национальную безопасность (ст. 24, 25).

И еще один важный аспект из общих правил поведения в информационном пространстве в процессе оборота цифровых данных предусмотрен ст. 10 рассматриваемого Закона: все участники делового, хозяйственного и т.д. оборота, отраслевые организации в соответствии со своими уставами должны разрабатывать свои «кодексы поведения и групповые стандарты безопасности данных, на основе закона укреплять самодисциплину в отрасли, направлять своих членов на совершенствование защиты безопасности данных, повышать уровень защиты безопасности данных, способствовать здоровому развитию отрасли».

Китайское государство в сфере безопасности и открытости правительственных данных, согласно ст. 39–43, вправе и обязано: создавать и совершенствовать систему управления безопасностью данных; получать другим лицам создавать и поддерживать систему электронного правительства, хранить и обрабатывать правительственные данные (ст. 44), но при этом контроль за этими лицами оставляет за собой; следовать в своей работе принципам справедливости, честности и удобства и раскрывать правительственные данные своевременно и точно, за исключением тех, которые не разглашаются в соответствии с Законом (ст. 41); разрабатывать открытый канал правительственных данных, создавать единую стандартизированную взаимосвязанную безопасную и контролируемую платформу для открытия правительственных данных (ст. 42).

Закон КНР о безопасности данных в гл. 6 уточняет, за что и в каких размерах накладываются штрафы на физические лица и организации за допущенные нарушения при обработке данных (максимально это не более 10 млн юаней). При этом соответствующий компетентный департамент может принимать и такие меры воздействия, как предписание исправить ситуацию; вынести

предупреждение; вынести постановление о приостановке соответствующей деятельности; отозвать соответствующее разрешение или лицензию на ведение предпринимательской деятельности и даже провести собеседование с соответствующими организациями и лицами и потребовать от них принятия мер по исправлению и устранению скрытых опасностей (ст. 44).

Закон КНР о безопасности данных предусматривает и другие штрафные санкции за нарушения в области безопасности и открытости правительственных данных (ст. 47–48). Дисциплинарные взыскания могут быть наложены на контролирующий и другой отвечающий непосредственно за работу персонал, если государственный орган не выполняет свои обязанности по защите безопасности данных.

Уголовной, административной ответственности должны быть подвергнуты те, кто «крадет или приобретает данные другими незаконными способами, осуществляет деятельность по обработке данных с целью исключения или наносит ущерб законным правам и интересам частных лиц или организаций» (ст. 51).

Не исключается гражданско-правовая ответственность за нарушения Закона о безопасности данных (ст. 52), а тех, кто нарушает управление общественной безопасностью ожидает административная ответственность.

Как и в Законе КНР о кибербезопасности, Закон КНР о безопасности данных содержит положение о том, что меры по защите безопасности военных данных должны быть отдельно сформулированы Центральной военной комиссией (ст. 54).

КНР: право на защиту персональных данных

Закон КНР о защите персональных данных принят Постоянным комитетом ВСНП 13го созыва 20.08.2021 г. и вступил в силу с 01.01.2022 г., т.е. всего на два месяца позже Закона КНР о безопасности данных. Этот Закон был принят на основе Конституции КНР в целях защиты прав и интересов в отношении персональных данных, стандартизации деятельности по их обработке и рациональному использованию (ст. 1).

«Персональные данные», согласно ст. 4 Закона, – «это все виды информации, записанные электронным или иным способом, относящиеся к идентификационному или идентифицирующемуся физическому лицу, за исключением информации, обработанной после анонимизации» (ст. 4).

Данный Закон содержит восемь глав, 74 статьи и декларирует: «персональные данные физических лиц охраняются законом, и никакая организация или частное лицо не могут нарушать права и интересы в отношении персональных данных физических лиц» (ст. 2); «персональные данные должны обрабатываться в соответствии с принципами законности, обоснованности, необходимости и честности» (ст. 5), а также «ни одна организация или частное лицо не должны незаконно собирать, использовать, обрабатывать или раскрывать персональные данные другого лица» (ст. 10).

Рассматриваемый Закон распространяет свое действие на обработку персональных данных китайских граждан за границей (ст. 10). Закон применяется в трех случаях: 1) в целях предоставления продуктов или услуг физическим лицам, находящимся на территории КНР; 2) при анализе и оценке поведения физических лиц, находящихся на территории КНР; 3) в других обстоятельствах, предусмотренных в законах или административных нормах Китая.

В гл. 1 «Общие положения» Закона КНР о защите персональных данных предусматривается: 1) «государство не только создает надежную систему защиты персональных данных и строго наказывает тех, кто это нарушает, но и усиливает пропаганду и просвещение в области защиты персональных данных, способствует формированию благоприятной среды, в которой правительство, предприятия, соответствующие общественные организации и население участвуют в защите персональных данных» (ст. 11); 2) готовность КНР активно участвовать на международном уровне: в разработке международных правил по защите персональных данных; их обмене и сотрудничестве; взаимном признании правил и стандартов, действующих в других странах и регионах; взаимодействии с международными организациями (ст. 12).

В гл. 2 (ст. 28–37) Закона устанавливаются правила обработки персональных данных[1]. Обработка персональных данных может работать с данными несовершеннолетнего в возрасте до 14 лет только получая согласие родителей или опекуна несовершеннолетнего (ст. 31).

Закон КНР о защите персональных данных в ст. 13 определяет семь обстоятельств, в связи с которыми обработчик может

[1] Под *обработкой персональных данных* ст. 73 данного Закона понимает «организацию или физическое лицо, которые самостоятельно принимают решение о цели и способах обработки персональных данных».

заниматься обработкой данных. Это получение согласия физического лица, когда оно необходимо для выполнения установленного законом полномочий или обязанностей, когда необходимо для заключения или исключения договора и в других случаях. Среди них есть такой: частичная обработка данных «в целях мониторинга общественного мнения и других действий в общественных интересах» (п. 5 ст. 13).

Чтобы приступить к обработке персональных данных (ст. 17), обработчик должен выполнить четыре условия, в том числе: «на видном месте и на ясном и понятном языке, правдиво, точно и полно информировать о своем наименовании и контактных данных, цели и порядке обработки персональных данных, сроки их хранения, правах и обязанностях физического лица, чьи данные обрабатываются». Обработчик персональных данных «не должен раскрывать обрабатываемые им персональные данные, кроме как с отдельного согласия физического лица» (ст. 25).

Анализируемый Закон в гл. 3 определяет условия и порядок передачи персональных данных за границу «в связи с деловыми или иными потребностями» (ст. 38). В связи с этим обработчик должен проходить оценку безопасности передаваемых данных (чем занимается Государственный департамент сетевой информации) либо иметь сертификат по защите персональных данных. При этом получатель данных за пределами КНР должен соответствовать стандартам защиты персональных данных, определяемых Законом КНР о защите персональных данных (ст. 38 Закона). Данные «критических инфраструктур» передаются обработчиком за пределы КНР только с разрешения Государственного департамента сетевой информации после проведения «оценки безопасности» (ст. 40).

Довольно подробно права физически лиц в процессе обработки и передачи персональных данных определены в гл. 4 Закона КНР о защите персональных данных (ст. 44–50). Главное состоит в том, что физическое лицо имеет право: знать и принимать решение об обработке персональных данных или отказаться от этого; проверять и копировать свои данные. Потребовать исправить или заменить собранные данные; отозвать свое согласие на сбор и обработку данных и т.д. Всё это, конечно, реализуется в рамках действующего в КНР законодательства.

Обязанности обработчиков персональных данных и госорганов, занимающихся их защитой, регулируются ст. 51–65 гл. 5 Закона КНР о защите персональных данных. Так, ст. 51 содержит

перечень требований к обработчику персональных данных, выполнение которых позволяет предотвратить незаконный доступ, а также утечку, фальсификацию и потерю данных. Среди них: разработка компанией-разработчиком данных внутренних систем управления и операционных процедур, внедрение классификационного управления персональными данными, принятия соответствующих технических мер безопасности и т.д. При этом устанавливается персональная ответственность лица, занимающегося непосредственно обработкой данных. Сведения о нем передаются в департамент, выполняющий обязанности по защите персональных данных (ст. 52).

Закон КНР о защите персональных данных требует от обработчика данных: провести предварительную оценку воздействия на защиту персональных данных и определить порядок, в том числе определить, являются ли принятые меры защиты законными, эффективными и соответствующими степени риска (ст. 56); немедленного принятия мер по исправлению ситуации при утечке, фальсификации и потере персональных данных (ст. 57).

Обязанности отраслевых департаментов, выполняющих работу по защите персональных данных (а они, как указывалось выше, действуют под руководством Государственного департамента сетевой информации), определены в ст. 61 Закона КНР о защите персональных данных: расследование и рассмотрение незаконных действий обработчиков данных; рассмотрение поступивших жалоб; проведение пропаганды и обучение по вопросам защиты персональных данных и др.

Данный Закон также предусматривает обязанности Государственного департамента сетевой информации, как то: разработка конкретных правил и стандартов для защиты персональных данных, поддержка исследований в данной области деятельности, содействие созданию системы специализированных услуг по защите персональных данных и др.

Права департаментов, выполняющих обязанности по защите персональных данных, включая право на проведение проверки бухгалтерских книг, опроса заинтересованных сторон, проведение проверок на местах и расследований проверки оборудования и т.д., определены в ст. 63 Закона.

Любая организация или частное лицо «имеют право подать жалобу или заявление о незаконной деятельности по обработке персональных данных в департаменты» (ст. 65), которые обязаны дать заявителю ответ. Сами же департаменты, выполняющие обя-

занности по защите персональных данных, «должны обнародовать конкретную информацию для получения жалоб и заявлений» (ст. 65).

Закон КНР о защите персональных данных в гл. 7 «Юридическая ответственность» (ст. 66–71) предусматривает ряд санкций, которые могут быть наложены на лицо, обрабатывающее персональные данные и нарушающее требования Закона: предупреждение; конфискация незаконных доходов; штраф в размере не более 1 млн юаней (на организацию); штраф не менее 10 тыс. юаней и не более 100 тыс. юаней (на контролирующий персонал и непосредственных исполнителей); приостановление деятельности; отзыв лицензии или разрешения на работу и др. (ст. 66).

При этом не исключается уголовная ответственность и занесение в кредитный рейтинг в соответствии с нормами административного права, а также предание гласности о случившейся ситуации (ст. 67).

На страже исполнения Закона КНР о защите персональных данных стоят не только сам обработчик данных, Государственный департамент сетевой информации и отраслевые департаменты, но и народная прокуратура, организации, определенные Государственным департаментом сетевой информации, которые имеют право в соответствии с законом обращаться в народные суды (ст. 71).

Заключение

В данном обзоре изложены основные положения трех законов Китайской Народной Республики – о кибербезопасности, о безопасности данных, о защите персональных данных, которые составляют правовой каркас «цифрового права» Китая. Его дополняют различного рода положения и временные меры, регулирующие деятельность сферы информационно-коммуникационных технологий, оборота персональных (и не только) данных, деятельность сетевых операторов, обработчиков данных, госорганов и т.д., утвержденных постановлениями Государственного совета КНР. Среди них ранее указанные: Положение о защите безопасности критической инфраструктуры 2021 г.; Временные меры по регулированию сервисов генеративного искусственного интеллекта 2023 г.; Положение об управлении рекомендациями для информационных интернет-услуг 2022 г.; Правила проверки кибербезопасности 2021 г. и др.