

Развитие законодательства КНР в области цифровой экономики

Китайская академия информационно-коммуникационных технологий (CAICT) опубликовала [«Белую книгу по киберзаконодательству \(2022\)»](#).

Белая книга по киберзаконодательству Китая представляет собой всеобъемлющий документ, в котором изложен подход страны к вопросам кибербезопасности и защиты персональных данных.

Исходя из количества и сути принятых в 2022 году актов, подход Китая к кибербезопасности заключается в принятии всеобъемлющих законов и нормативных актов, которые должны быть четкими и легко выполнимыми, а также в создании эффективных механизмов контроля и обеспечения соблюдения принимаемых актов.

Кроме того, наблюдается тенденция регламентации сотрудничества между правительством, промышленностью и другими заинтересованными сторонами для обеспечения эффективности принимаемых законов и подзаконных актов. Такой подход видится целесообразным поскольку кибербезопасность является глобальной и важной проблемой, для эффективного решения которой необходимы скоординированные усилия госорганов, отрасли и пользователей. Одним из ключевых направлений Белой книги является защита персональных данных. Поскольку сбор и использование персональных данных становится все более распространенным явлением в эпоху цифровизации, существует необходимость во всеобъемлющих законах и нормативных актах для защиты прав пользователей.

Для решения этих проблем в Белой книге изложен ряд мер, которые Китай принял в 2022 году и планирует принять в 2023 году. К ним относятся создание национальной системы защиты персональных данных, разработка стандартов и руководящих принципов для сбора и использования персональных данных, а также создание системы рассмотрения жалоб и споров, связанных с персональными данными.

В Белой книге также рассматривается вопрос киберпреступности, поскольку с повсеместной цифровизацией появляются более изощренные методы совершения преступлений онлайн (связанные не только с мошенничеством). В документе описан ряд мер, которые Китай планирует принять в 2023 году в рамках борьбы с киберпреступностью, включая создание специализированных агентств по борьбе с киберпреступностью, разработку комплексных законов и нормативных актов, а также создание механизмов международного сотрудничества.

Содержание Белой книги позволяет сделать вывод о том, что для эффективного регулирования ИТ-сферы необходимо сочетание двух факторов:

- 1) системность и исполнимость регулирования;
- 2) сотрудничество государства и отрасли.

Их наличие позволяет Китаю создавать гармоничную среду для развития ИТ-отрасли, в том числе в условиях усиления киберугроз.

Далее будут представлены некоторые выдержки из Белой книги по направлениям принимаемых актов.

I. Трансграничное управление данными

В июне 2022 года был опубликован для обсуждения проект *Положения о типовых договорах на персональную информацию*, в котором разъясняется сфера применения предоставления персональной информации за пределами Китая путем заключения типовых договоров, их содержание и пример текста типовых договоров.

Текст типового договора содержит положения об обязанностях обработчика персональных данных, обязанностях получателя за пределами КНР, а также о правах субъекта персональных данных. Отмечается, что типовые договоры основаны на Законе о защите личной информации и, опираясь на развитую международную практику (ЕС и АСЕАН), предусматривают соответствующее содержание, адаптированное к потребностям граждан КНР.

В феврале 2023 года был опубликован финальный текст предлагаемых мер, которые вступят в силу 1 июня 2023 года.

В июле 2022 года Государственное управление интернет-информации приняло *Меры по оценке безопасности экспорта данных* (в силе с 1 сентября 2022 года). Документ уточняет процесс и требования к оценке безопасности экспорта данных, а также создает правовую основу для функционирования механизма по экспорту данных. В частности, Меры содержат положения в отношении целей оценки, процессов оценки и регулирующих органов. Также уточняются сценарии, требующие предоставления данных за пределами страны путем оценки безопасности.

II. Безопасность данных

Закон о безопасности данных КНР определяет ответственность Министерства промышленности и информационных технологий за надзор за безопасностью данных в промышленном и телекоммуникационном секторах, а также устанавливает соответствующие требования к обязательствам по защите безопасности для обработчиков данных.

8 декабря 2022 года Министерство промышленности и информационных технологий после двух раундов общественных консультаций опубликовало окончательный текст *Временных административных мер по обеспечению безопасности данных в промышленности и информационных технологиях*, ставшие первым отраслевым нормативным актом по режиму безопасности данных, который предлагалось установить Законом о безопасности данных.

Меры охватывают следующие аспекты: 1) определение понятий «данные» и «обработчик данных в сфере промышленности и информационных технологий», 2) уточнение сфер надзора и надзорных обязанностей; 3) определение требований, связанных с классификацией данных; 4) уточнение и разъяснение требований по защите безопасности для всех категорий данных; 5) уточнение рабочих механизмов для мониторинга безопасности данных и предупреждения утечек.

III. Кибербезопасность

В январе 2022 года были приняты *Меры по цензуре сетевой безопасности*, которые вступили в силу 15 февраля 2022 года. Документ был разработан Государственным управлением интернет-информации совместно с 13 другими ведомствами.

Увеличено количество целей для проверки безопасности, условиями для инициирования проверки являются факторы, «влияющие или способные повлиять на национальную безопасность».

Также был расширен перечень регуляторов: в дополнение к предыдущим двенадцати ведомствам в качестве нового регулятора по проверке кибербезопасности была добавлена Комиссия по регулированию ценных бумаг Китая.

В сентябре 2022 года Государственное управление интернет-информации опубликовало для общественных консультаций проект *Решения о внесении изменений в Закон о сетевой безопасности Китайской Народной Республики*. Поправки касаются совершенствования системы ответственности за нарушение общих положений безопасности эксплуатации сети. В частности, предлагается изменить ответственность за обеспечение безопасности критической информационной инфраструктуры (КИИ). Также предлагаются изменения ответственности за нарушения в области защиты персональных данных.

В случае принятия, Решение станет первым пакетом поправок к Закону о кибербезопасности с момента его вступления в силу в 2017 году.

IV. Защита критической информационной структуры

В апреле 2022 года Комиссия по регулированию ценных бумаг опубликовала проект обновленных *Мер по управлению кибербезопасностью в индустрии*

ценных бумаг и фьючерсов. Окончательный текст был представлен в феврале 2023 года, Меры вступят в силу 1 мая 2023 года.

Меры охватывают различные аспекты сетевой и информационной безопасности, такие как создание и функционирование систем надзора и управления, защита личной информации инвесторов, реагирование на чрезвычайные ситуации в области сетевой и информационной безопасности, защита безопасности критической информационной инфраструктуры (добавлена отдельная глава «Критическая информационная инфраструктура»).

В августе Министерство транспорта и коммуникаций разместило для публичных консультаций проект *Мер по управлению защитой безопасности критической информационной инфраструктуры на автомагистралях и водных путях.*

Меры содержат 48 статей, которые предусматривают идентификацию критической информационной инфраструктуры автомобильных и водных путей, ответственность и обязательства оператора, вспомогательные и надзорные меры.

В декабре Национальное энергетическое бюро опубликовало принятые *Меры по управлению сетевой безопасностью в электроэнергетике* и *Меры по управлению защитой уровня сетевой безопасности в электроэнергетике*, которые содержат подробные положения о сетевой безопасности в электроэнергетике и требуют, чтобы операторы КИИ в электроэнергетике уделяли приоритетное внимание закупке безопасных и надежных сетевых продуктов и услуг, а также проводили работу по предварительному определению рисков.

V. Сетевая экология

В апреле 2022 года было опубликовано *Уведомление об усилении управления прямыми трансляциями игр на платформах сетевых аудиовизуальных программ*.

Документ представляет из себя руководящие принципы по регулированию прямых трансляций в Интернете и усилению защиты несовершеннолетних. Предлагаются меры по запрету участия несовершеннолетних в прямых трансляциях, по строгому контролю несовершеннолетних в качестве ведущих, по усилению управления в часы пик и повышению качества образования в Интернете.

В мае 2022 года Государственная администрация радио и телевидения опубликовала *Административные меры по управлению брокерскими агентствами в области радио, телевидения и интернет-аудиовизуальных программ*, требующие от брокерских агентств получения соответствующей квалификации. Мерами предусмотрено, что один и тот же брокер может предоставлять услуги не более чем 100 исполнителям. Меры вступили в силу 30 июня 2022 года.

В августе Государственная администрация радио и телевидения выпустила проект *Административного регламента по производству и эксплуатации радио, телевидения и аудиовизуальных программ в Интернете*, который распространяется на аудиовизуальный контент и регулирует деятельность посредников и поставщиков услуг в сфере аудиовизуального контента.

В июне 2022 года Государственное управление интернет-информации пересмотрело и опубликовало *Положение об администрировании информационных услуг мобильных приложений*, которое требует, чтобы поставщики приложений и платформы их распространения несли ответственность за управление информационным содержанием приложений. Среди прочего, поставщики приложений должны проводить аутентификацию по реальному имени, осуществлять управление информационным контентом, запрещать недобросовестную конкуренцию, гарантировать безопасность приложений и собираемых ими данных, защищать персональные данные,

защищать несовершеннолетних, проводить оценку безопасности новых технологий и приложений и осуществлять управление счетами.

Положение вступило в силу 1 августа 2022 года.

В сентябре опубликовано *Положение об управлении услугами по продвижению всплывающей в Интернете информации* (пуш-уведомлений), согласно которому поставщики услуг по продвижению пуш-уведомлений должны выполнять основную ответственность за управление информационным содержанием, усилить аудит содержания пуш-уведомлений и воздерживаться от продвижения незаконной и нежелательной информации.

Положение вступило в силу 30 сентября 2022 года.

В декабре 2022 вступили в силу пересмотренные *Правила управления службами комментирования в Интернете*, в которых рассматриваются новые ситуации и вопросы, возникающие в связи со службами комментирования в Интернете, и уделяется особое внимание разъяснению обязанностей поставщиков услуг комментирования, пользователей услуг комментирования и производителей и операторов публичных аккаунтов.

VI. Борьба с мошенничеством с использованием телекоммуникационных сетей

В апреле 2022 года Генеральный аппарат ЦК КПК и Генеральный аппарат Госсовета опубликовали *Уведомление об усилении работы по борьбе и противодействию незаконным преступлениям в телекоммуникационных сетях*.

В сентябре был официально представлен *Закон о борьбе с мошенничеством в телекоммуникационных сетях*, который вступил в силу 1 декабря 2022 года. Закон определяет, что является мошенничеством в телекоммуникационных сетях, сферу применения закона, меры управления в ключевых областях, таких как телекоммуникации, финансы и Интернет.

VII. Антимонопольные инициативы: недобросовестная конкуренция с участием онлайн-платформ

В июне 2022 года Постоянный комитет Всекитайского собрания народных представителей проголосовал за принятие *Решения о внесении изменений в Закон о борьбе с монополиями*. Уточняется, что операторы не должны злоупотреблять данными и алгоритмами, технологиями, преимуществами капитала и правилами платформы для исключения или ограничения конкуренции. Злоупотреблением доминирующим положением на рынке считается, если оператор использует данные и алгоритмы, технологии и правила платформы для наложения необоснованных ограничений на других операторов. Поправки вступили в силу 1 августа 2022 года.

В ноябре Государственная администрация по надзору и регулированию рынка опубликовала проект *Закона о борьбе с недобросовестной конкуренцией*. Пересмотренный проект учитывает особенности конкуренции в цифровой экономике и содержит подробные положения о недобросовестной конкуренции при получении и использовании данных, недобросовестной конкуренции, совершаемой с помощью алгоритмов, и новых видах недобросовестной конкуренции в Интернете. Кроме того, предусматривается усиленная ответственность операторов платформ. Законопроект все еще находится на рассмотрении.

VIII. Алгоритмы

Первым аспектом в данном направлении является всеобъемлющее регулирование рекомендательных сервисов, основанных на алгоритмах. В марте 2022 года вступило в силу *Положение об администрировании алгоритмических рекомендаций информационных интернет-услуг*, которое устанавливает всеобъемлющее регулирование технологии алгоритмических рекомендаций информационных интернет-услуг в Китае. Положение включает все услуги технологии алгоритмических рекомендаций, в том числе

генерацию и синтез, персонализированное продвижение, сортировку и выбор, поиск и фильтрацию, планирование и принятие решений и т.д., в сферу регулирования закона. Устанавливаются такие обязательства, как оценка алгоритмов.

Предусматривается трехуровневая система защиты прав и интересов пользователей: защита персональных данных пользователей, обеспечение прозрачности алгоритмов и механизмов независимого выбора пользователей, требование надлежащего раскрытия основных принципов, целей и основных рабочих механизмов рекомендательных алгоритмов, а также обеспечение отказа от рекомендаций алгоритмов, управление метками пользователей, обязательства по описанию и разъяснению алгоритмов.

Кроме того, Положение предусматривает обеспечение равных прав и интересов пользователей, а также обеспечение того, что алгоритмы не должны использоваться для реализации необоснованного дифференцированного подхода к ценам и другим условиям сделок.

В декабре Государственное управление интернет-информации, Министерство промышленности и информационных технологий и Министерство общественной безопасности совместно опубликовали *Положения об управлении глубоким синтезом информационных услуг в Интернете*. Положение предусматривает основные руководящие принципы и правовую основу для развития глубокого синтеза (т. н. «дипфейки») информационных услуг в Интернете. Правила глубокого синтеза требуют от поставщика услуг глубокого синтеза создания и совершенствования системы управления механизмом алгоритмов, аудита механизма, управления информационным содержанием, обучения и подготовки специалистов. Правила вступили в силу 10 января 2023 года.

IX. Беспилотные автомобили

Министерство промышленности и информационных технологий выпустило ряд проектов для уточнения требований к управлению умными автомобилями.

Министерство опубликовало проект *Положения о лицензировании доступа к производству дорожных транспортных средств*, где определены специальные требования к управлению беспилотными автомобилями: 1) наличие лицензии на производство таких транспортных средств; 2) гарантии сетевой безопасности транспортного средства; 3) обеспечение безопасности данных.

Также был опубликован проект *Уведомления о пилотной работе по доступу беспилотных автомобилей в рамках национального проекта по дорожным испытаниям и демонстрационному применению беспилотных автомобилей*, в котором предлагается содержание доступа и дорожного доступа. Для участия в эксперименте отобраны производители транспортных средств, оснащенных функцией автопилота, которые могут быть допущены к серийному производству. Эксперимент будет проведен на дорогах общего пользования в ограниченных зонах в некоторых городах.