

УДК 338.23 DOI: 10.14451/1.222.416

Механизмы управления и правовые гарантии безопасности цифровой экономики Китая

© 2023 Юэлун Чжан

Аспирант Институт бизнеса БГУ E-mail: bsuzhang@gmail.com

Ключевые слова: цифровая экономика, Китай, персональные данные, кибербезопасность, правовое регулирование, цифровые технологии.

Реализуя приоритеты развития информационной экономики Китая, определенные XX съездом Коммунистической партии Китая, решая, поставленную Председателем КНР Си Цзиньпином задачу «всестороннего усиления государственной безопасности», в части цифровой экономики Китай успешно реализует положения «Стратегии национальной безопасности в киберпространстве», в развитие которой принят комплекс законов, в том числе о кибербезопасности и персональных данных, сформированы и запущены соответствующие механизмы управления.

Признав цифровую трансформацию главной силой реструктуризации глобальной экономики, председатель КНР Си Цзиньпин, призвал к расширению национальной цифровой экономики через глубокую интеграцию цифровых технологий в реальную экономику, а также их применение, как в модернизации традиционных отраслей, так и в развитии новых. Именно «уверенный рост цифровой экономики», отметил председатель КНР, обеспечит Китаю продвижение новой парадигмы развития, содействуя новым конкурентным преимуществам. В числе задач лидер Китая отметил приоритет автономности в производстве технологий, самостоятельности в реализации инноваций, опираясь на социалистическую систему и крупнейший в мире внутренний рынок. Все эти задачи могут быть решены, как отметил Си Цзиньпин, на базе ускорения формирования новой инфраструктуры, в рамках которой заработает информационная «артерия» экономического и социального развития [7].

Российские эксперты высоко оценивают темпы роста основных показателей развития цифровой экономики Китая в 2018-2022 годах, считая, что они за указанный период превышают 25%. Э.В. Горян отметила акцент на государственно-частном партнерстве как преимуществу китайской стратегии кибербезопасности, противопоставив её российской практике, где, по мнению цитируемого автора, «основная ответственность возложена на государственно-публичный сектор» [2, с. 118].

В 2022 г. Китай занял лидирующие позиции в сферах электронной торговли, финансовых технологиях, облачных вычислениях, а также в экспорте IT-продукции. Стабильно растут и позиции Китая в международных цифровых рейтингах: Индексах мировой цифровой конкурентоспособности (17 позиция в 2022 г. [10]) и развития электронного правительства. В Рейтинге Глобального инновационного индекса 2022 г. Китай занял 11 место из 132 стран [1].

В числе факторов высокой мировой цифровой конкурентоспособности Китая принято называть: практически неисчерпаемый потенциал внутреннего рынка, высокий уровень технологий, активное государственное стимулирование инноваций, развитие высокотехнологичных китайских корпораций, качество образования и результатов НИОКР [6, с. 30].

Принимая во внимание глубокое цифровое проникновение, особенно после пандемии COVID-19, всё более активное участие населения в апробации и использовании новых технологий и возможностей, рост инвестиций в цифровую трансформацию требуют формирования надлежащей институциональной среды, в рамках которой должна быть обеспечена безопасность стремительно развивающихся информационных процессов.

В 2022 г. Китайская академия информационно-коммуникационных технологий (CAICT) выпустила «Белую книгу по киберзаконодательству», где прослеживается государственный и частный подходы к сферам кибербезопасности, защиты персональных данных [9]. Правовая политика Китая в сфере кибербезопасности в 2022 г. заключалась в пополнении и систематизации нормативной правовой базы формирования эффективных механизмов реализации и контроля правоприменения, а также развитии положений Закона о кибербезопасности 2017 г. [3]

Существенное ужесточение стандартов кибербезопасности в Китае после 2017 г. в части требований к компаниям открывать свои сети и устанавливать одобренное правительством оборудование, вызвали обеспокоенность за рубежом, прежде всего, в США, чьи компании считают это чрезвычайным обременением [11], создающим «целый ряд новых сложностей, особенно для компаний-разработчиков программного обеспечения за пределами Китая». Американские компании опасаются утраты своей конфиденциальной информации о бэкдорах и т. д. и даже грозят исключить китайских экспертов в области безопасности из международных программ [8]. Такая реакция демонстрирует внеш-

нюю заинтересованность Запада в слабости и уязвимости компьютерной безопасности Китая, усиление которой сразу вызвала тревогу.

Несмотря на внешнее давление китайское правительство в 2022 г. последовательно и настойчиво проводило политику ужесточения правового режима кибербезопасности, перекрывая любые лазейки для противоправных посягательств и угроз национальной безопасности в цифровом пространстве.

В 2022 г. продолжалась тенденция детальной регламентации кооперации правительства, бизнеса и прочих заинтересованных сторон для обеспечения правовой эффективности. Белая книга CAICT 2022 г. в основном ориентирована на защиту персональных данных, сбор, хранение, накопление и использование которых стали одним из основных направлений деятельности операторов и агрегаторов больших объемов данных.

Книга содержит события и меры 2022 г., а также планы на 2023 г. в сфере формирования национальной системы защиты персональных данных, подготовки и утверждения стандартов и руководящих принципов в сфере персональных данных, разработки действенной системы рассмотрения жалоб и разрешения споров по персональным данным.

В Белой книге CAICT 2022 г. значительное место уделено киберпреступности, особенно правовой политике Китая в этой сфере в 2023 г., в том числе учреждению в новых специализированных институтов – специализированных агентств по противодействию киберпреступности, разработке профильного законодательства, в том числе и в деле развития механизмов международного сотрудничества.

Вопросы, поставленные в Белой книге CAICT 2022 г. построены на представлении о том, что эффективное регулирование цифровой среды требует учёта нескольких факторов. Во-первых, детального знания и понимания процессов и общественных отношений, развивающихся в этой сфере. Во-вторых, системного подхода

к правотворчеству, с учётом реальной исполнимости требований принимаемых законов. В-третьих, кооперации государства и IT-отрасли. В-четвертых, соответствия международным требованиям в регулируемой сфере, что особенно касается вопросов безопасности.

В условиях сложной международной обстановки, угроз терроризма и киберпреступности важно обеспечить пресечение и превенцию противоправного трансграничного управления данными. С этой целью в июне 2022 г. китайское правительство опубликовало для публичного обсуждения проект Положения о типовых договорах на персональную информацию, где был изложен порядок её предоставления и обработки за пределами Китая, посредством составления типовых договоров, которые включали статьи об обязанностях оператора персональных данных, обязанностях их иностранного субъекта. Собственно сами типовые договоры, строго говоря, не являются новеллой китайского законодательства, так как подготовлены на базе Закона о защите личной информации [4], а также международном (мягком) праве и практике, но адаптированы к китайскому законодательству и институтам. В феврале 2023 г. правительство опубликовало окончательный перечень нормативных установлений, запланировав их вступление в силу 1 июня 2023 г.

1 сентября 2022 г. вступили в силу разработанные Государственным управлением интернет-информации «Меры по оценке безопасности экспорта данных» (数据出境安全评估办法), где были регламентированы процедуры и требования к оценке безопасности экспорта данных. Также документ обеспечил правовую базу механизму экспорта данных и систематизировал основные сегменты: цели, процессы оценки, а также права контролирующих (надзорных органов) [5]. Кроме того, в «Мерах» детализованы ситуации возникновения потребности в предоставлении персональных данных за границу, в части обеспечения безопасности этой процедуры.

В части охраны безопасности данных китайский Закон о безопасности данных возлагает

на Министерство промышленности и информационных технологий функции надзор за этой сферой в промышленности и секторе телекоммуникаций на основе обязательных требований к операторам данных. Важно, что вступившие в силу 8 декабря 2022 г. «Временные административные меры по обеспечению безопасности данных в промышленности и информационных технологиях», став первым нормативным актом, регламентирующим безопасность данных, из числа планируемых к разработке в рамках реализации положений Закона о безопасности данных, были приняты Министерством после интенсивных общественных консультаций.

В «Мерах» даны легальные определения ключевых понятий, оперируемых в регулируемой сфере: «данные» и «оператор данных в сфере промышленности и информационных технологий». Также в документе точно прописаны сферы и полномочия надзора, приведены классификация данных; требования по обеспечению их безопасности, дифференцировано по видам, а также порядок мониторинга безопасности данных и предупреждения их утраты, повреждения или хищения.

В развитие положений Закона о кибербезопасности КНР от 7 ноября 2016 г. [12] в январе 2022 г. были введены «Меры по цензуре сетевой безопасности» (вступили в силу 15 февраля 2022 г.), ставшие результатом межведомственного взаимодействия Государственного управления интернет-информации и ещё 13 государственных структур. Документ предусматривает существенную диверсификацию как целей проверки безопасности, так поводов, оснований и условий её проведения. При этом основаниями могут стать факторы, «влияющие или способные повлиять на национальную безопасность». В документе расширено число государственных структур, полномочных осуществлять надзор в сфере кибербезопасности. Если ранее их было 12, то сейчас добавилась Комиссия по регулированию ценных бумаг.

Реализуя практику публичного обсуждения проектов нормативных актов, затрагивающих ин-

формационные права, Государственное управление интернет-информации в сентябре 2022 г. вынесло на общественные консультации проект своего «Решения о внесении изменений в Закон о сетевой безопасности», где речь шла о корректировке ответственности за нарушение регламентов по безопасности эксплуатации сети. Так, была ужесточена ответственность за поддержание безопасности критической информационной инфраструктуры. То же касалось и ответственности за нарушения в сфере защиты персональных данных. Примечательно (не характерно для России), что Решение стало первым пакетом поправок к Закону о кибербезопасности 2016 г.

В части защиты критической информационной структуры Комиссия по регулированию ценных бумаг разработала проект уточненных «Мер по управлению кибербезопасностью в индустрии ценных бумаг и фьючерсов», которые вступили в силу 1 мая 2023 г. В документе регламентируются несколько аспектов обеспечения сетевой и информационной безопасности. Прежде всего, это надзор и управление, защита личной информации инвесторов, реагирование на чрезвычайные ситуации, защита безопасности критической информационной инфраструктуры, в этой части ранее действовавшие «Меры» были дополнены новой, теперь отдельной главой.

Аналогичный документ в пределах своей сферы ответственности в августе 2022 г. разработало Министерство транспорта и коммуникаций, также опубликовав проект «Мер по управлению защитой безопасности критической информационной инфраструктуры на автомобильных дорогах и водных путях» в составе 48 статей. Документ идентифицирует отраслевые признаки критической информационной инфраструктуры, регламентируя ответственность и обязательства оператора, а также порядок и полномочия надзора.

Аналогичный документ был обнародован Национальным энергетическим бюро в декабре 2022 г. В данном случае «Меры по управлению сетевой безопасностью в электроэнергетике» и «Меры по управлению защитой уровня сетевой

безопасности в электроэнергетике», включали соответствующие отраслевые положения, а также требования к операторам КИИ в электроэнергетике о выборе безопасных и проверенных сетевых продуктов и услуг.

В апреле 2022 г. Государственное управление интернет-информации Китая издало «Уведомление об усилении управления прямыми трансляциями игр на платформах сетевых аудиовизуальных программ», разработанное в целях защиты несовершеннолетних от возможного негативного воздействия. В данном случае был введен запрет на участие несовершеннолетних в прямых трансляциях, а также их допуску как ведущих. Параллельно были приняты меры к ужесточению требований к качеству онлайн образования.

30 июня 2022 г. вступили в силу разработанные Государственной администрацией радио и телевидения «Административные меры по управлению брокерскими агентствами в области радио, телевидения и интернет-аудиовизуальных программ», в соответствии с которыми были введены обязательные квалификационные требования к брокерам.

В августе 2022 г. Государственная администрация радио и телевидения издала проект «Административного регламента по производству и эксплуатации радио, телевидения и аудиовизуальных программ в Интернете», распространив его на аудиовизуальный контент. Документ также регламентировал деятельность посредников и поставщиков услуг в указанной сфере.

1 августа 2022 г. вступило в силу «Положение об администрировании информационных услуг мобильных приложений», разработанное Государственным управлением интернет-информации. Документ корректировал ранее действовавшее Положение, вводя ответственность поставщиков приложений и платформ за их содержанием.

В частности, поставщиков обязали исключить никнеймы, проводить строгую аутентификацию по реальным персональным данным, управлять информационным контентом. Поставщик обязан

гарантировать безопасность приложений, соблюдать конфиденциальность обрабатываемых ими данных и защищать их от несанкционированного доступа.

30 сентября 2022 г. вступило в силу «Положение об управлении услугами по продвижению всплывающей в Интернете информации (пуш-уведомлений)», в соответствии с которым поставщики соответствующих услуг несли ответственность за информационное наполнение, пресекая продвижение незаконной и нежелательной для пользователей информации.

В декабре 2022 г. были скорректированы «Правила управления службами комментирования в Интернете», где были регламентированы обязанности поставщиков и пользователей соответствующих услуг.

Сферой особого внимания китайских законодателя и регуляторов в 2022 г. оставалась противодействие мошенничеству в Интернете. В апреле того же года Генеральный аппарат ЦК КПК и Генеральный аппарат Госсовета издали «Уведомление об усилении работы по борьбе и противодействию незаконным преступлениям в телекоммуникационных сетях», а к сентябрю был разработан Закон КНР «О борьбе с мошенничеством в телекоммуникационных сетях» (вступил в силу 1 декабря 2022 г.). Правоприменитель получил определение «мошенничества в телекоммуникационных сетях», была определена сфера применения закона.

Принимая во внимание высокие темпы развития китайской экономики особую актуальность имеет антимонопольное регулирование в цифровой среде. В данном случае речь идет об обеспечении безопасности торгов и процедур на онлайн-платформах.

В июне 2022 г. Постоянный комитет Всекитайского собрания народных представителей принял поправки к Закону о борьбе с монополиями, в соответствии с которыми операторы не вправе злоупотреблять данными, алгоритмами, технологиями, как и статусом платформы для создания помех конкуренции.

В соответствии с Законом злоупотребление доминирующим положением на рынке фиксируется, когда оператор использует данные и алгоритмы, технологии и правила платформы в целях создания помех работе других операторов, т. е. помешать конкуренции.

Таким образом, в плане реализации положений Стратегии национальной безопасности в киберпространстве КНР в совокупности законодательства о кибербезопасности и персональных данных, институализованы правовые гарантии безопасности цифровой экономики Китая. Механизмы управления в этой сфере выстроены на базе приоритета задач национальной безопасности с учётом частного интереса китайских компаний, а также позиции заинтересованного сообщества, которое привлекается к обсуждению законопроектов.

Библиографический список

1. Глобальный инновационный индекс. — 2022. — URL: <https://globalstocks.ru/wp-content/uploads/2022/10/wipo-pub-2000-2022-exec-ru-global-innovation-index-2022-15th-edition.pdf>.
2. Горян Э. В. Нормативно-правовая основа обеспечения национальной безопасности в киберпространстве: опыт Китайской Народной Республики // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. — 2021. — Вып. 13, № 1. — С. 115–124.
3. Закон Китайской Народной Республики о кибербезопасности. Принят Постоянным комитетом Всекитайского собрания народных представителей 7 ноября 2016 г.
4. Закон о защите частной информации (PIPL). Принят Постоянным комитетом 13-го Всекитайского собрания народных представителей 20 августа 2021 г. — URL: https://translated.turbopages.org/proxy_u/en-ru.ru.5624e13d-644b6722-e9bd5a5e-74722d776562/en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm.
5. Китай принимает меры по оценке безопасности экспорта данных. — URL: <https://ru.chinajusticeobserver.com/a/china-issues-measures-for-data-export-security-assessment>.

6. Левченко Т. А. Цифровая экономика Китая: уровень и факторы развития // Вестник Астраханского государственного технического университета. Серия: Экономика. — 2021. — № 3. — С. 28–36.
7. Лидер цифры. Как Китай «оцифровывает» свою экономику / РИА «Новости». — 2021. — URL: <https://ria.ru/20211229/kitay-1766052437.html>.
8. Arjun Ramprasad China lays down new vulnerability disclosure rules / Previewtech.net. — 2021. — URL: <https://previewtech.net/china-lays-down-new-vulnerability-disclosure-rules>.
9. CAICT 2022 AI White Paper. — URL: <http://www.caict.ac.cn/kxyj/qwfb/bps/202204/P020220412613255124271.pdf>.
10. The 2022 IMD World Digital Competitiveness Ranking. — URL: <https://www.imd.org/centers/wcc/world-competitiveness-center/rankings/world-digital-competitiveness-ranking>.
11. Uchill Joe China's upgraded cybersecurity law could take a toll / Axios. — 2019. — URL: <https://www.axios.com/2019/10/17/china-cybersecurity-law-upgrade>.
12. 中华人民共和国网络安全法. — URL: <https://baike.baidu.com/item/16843044?fr=aladdin>.