

УДК 34.05(5+4-15):004

doi:10.35853/vestnik.gu.2025.13-3.09

5.1.1

Сравнительный анализ цифрового законодательства стран Азии и Западной Европы

Анатолий Борисович Чиквин

Уральский институт управления Российской академии народного хозяйства и государственной службы при Президенте РФ, Екатеринбург, Россия, anatolle@mail.ru

Аннотация. Цель исследования – выявить ключевые тенденции и особенности цифрового законодательства стран Азии и Западной Европы для разработки рекомендаций по модернизации российской правовой системы. В качестве объекта анализа выбраны законодательные акты и стратегические документы Италии, Франции, Германии, Великобритании, США (западная группа), а также Китая, Индии и Сингапура (азиатская группа). Методологическую основу составили сравнительно-правовой анализ, системный подход к изучению нормативных текстов, классификация стран по региональному признаку, синтез общих принципов и критическая оценка регуляторных противоречий. Результаты исследования демонстрируют, что западные страны фокусируются на правах граждан, децентрализованном управлении и балансе между открытостью данных и их защитой. В азиатских государствах доминируют централизованный контроль, приоритет национальной безопасности и жесткое регулирование новых технологий. Общими чертами для всех стран стали цифровизация госуслуг, меры кибербезопасности и риски, связанные с ресурсными ограничениями и бюрократией. Выявленные противоречия включают конфликт между инновациями и регуляторными барьерами, неоднозначность терминологии и пробелы в регулировании трансграничных данных. На основе проведенного анализа предложены рекомендации для России: интеграция западного опыта в сфере прозрачности и защиты прав граждан с азиатскими подходами к безопасности и технологическому суверенитету. Подчеркивается необходимость гибкого регулирования, инвестиций в инфраструктуру и обучения госслужащих для устойчивой цифровой трансформации.

Ключевые слова: цифровое законодательство, сравнительный анализ, кибербезопасность, цифровизация госуслуг, регуляторные противоречия, технологический суверенитет

Для цитирования: Чиквин А. Б. Сравнительный анализ цифрового законодательства стран Азии и Западной Европы // Вестник Гуманитарного университета. 2025. Т. 13, № 3. С. 142–153. DOI 10.35853/vestnik.gu.2025.13-3.09.

Comparative Analysis of Digital Legislation in Asia and Western Europe

Anatolii B. Chikvin

Ural Institute of Management, Russian Academy of National Economy and Public Administration under the President of the Russian Federation, Yekaterinburg, Russia, anatolle@mail.ru

Abstract. The objective of the study is to identify key trends and features of digital legislation in Asian and Western European countries to develop recommendations for modernizing the Russian legal system. The objects of analysis include legislative acts and strategic documents of Italy, France, Germany, Great Britain, the USA (Western group), as well as China, India and Singapore

(Asian group). The methodological basis is a comparative legal analysis, a systems approach to the study of regulatory texts, classification of countries by region, synthesis of general principles and a critical assessment of regulatory contradictions. The results of the study demonstrate that Western countries focus on the rights of citizens, decentralized governance and the balance between openness of data and its protection. In Asian countries, centralized control, priority of national security and strict regulation of new technologies dominate. Common features for all countries are the digitalization of public services, cybersecurity measures and risks associated with resource constraints and bureaucracy. The identified contradictions include the conflict between innovation and regulatory barriers, ambiguity of terminology and gaps in the regulation of cross-border data. Based on the analysis, recommendations are proposed for Russia: integration of Western experience in the field of transparency and protection of citizens' rights with Asian approaches to security and technological sovereignty. The need for flexible regulation, investment in infrastructure and training of civil servants for sustainable digital transformation is emphasized.

Keywords: digital legislation, comparative analysis, cybersecurity, digitalization of public services, regulatory conflicts, technological sovereignty

For citation: Chikvin AB. Comparative Analysis of Digital Legislation in Asia and Western Europe. *Vestnik Gumanitarnogo universiteta = Bulletin of Liberal Arts University*. 2025;13(3):142-153. (In Russ.). DOI:10.35853/vestnik.gu.2025.13-3.09.

Введение

В условиях глобальной цифровизации формирование эффективного законодательства, регулирующего цифровую среду, становится ключевым вызовом для государств. Различия в подходах к управлению данными, кибербезопасности, защите прав пользователей и внедрению инноваций отражают не только правовые традиции, но и стратегические приоритеты стран. Сравнительный анализ цифрового законодательства позволяет выявить универсальные тенденции, региональные особенности и оптимальные модели регулирования, что особенно актуально для России, стоящей перед необходимостью модернизации правовой базы в контексте технологических вызовов.

С 2014 года в России обсуждается вопрос о создании Цифрового, или Информационного, кодекса. Предпринимаются различные попытки принятия такого законодательного акта и в других странах СНГ: Казахстане, Кыргызстане, Узбекистане (см., напр.: [Цифровой кодекс Кыргызской Республики 2024]). Модельный кодекс в этой области принят Межпарламентской ассамблеей государств-участников СНГ [Модельный Информационный кодекс ... 2022].

В этой связи особенно интересно, как аналогичные задачи решались в других странах, какие подходы при этом использовались в зависимости от правовой традиции, с какими трудностями столкнулись разработчики. Необходимо отметить, что в той или иной степени свое законодательство, регулирующее отношения в цифровой сфере, есть во многих странах.

Насколько нам известно, до сих пор не предпринималось попыток провести сравнительный анализ цифрового законодательства в таком аспекте. Приступая к исследованию, мы выдвигаем гипотезу, что, несмотря на различия в правовых традициях и приоритетах, цифровое законодательство стран Западной Европы и Азии демонстрирует ряд универсальных принципов, связанных с цифровизацией госуслуг, защитой данных и балансом между свободой и контролем. Комплексное сопоставление законодательств двух региональных групп позволяет не только констатировать различия, но и выявить взаимодополняющие элементы.

Мы исходим из того, что комбинация подходов западных стран (их акцент на правах граждан) и азиатских (их приоритетное внимание к безопасности и к суверенитету) может стать основой для формирования гибкой и устойчивой правовой системы в России.

Таким образом, объектом исследования выступают законодательные акты и стратегические документы, регулирующие цифровую сферу в странах дальнего зарубежья: Италии, Франции, Германии, Великобритании, США (западная группа), а также в Ки-

тае, Индии и Сингапуре (азиатская группа). Предмет исследования включает сущность этих документов с акцентом на их структуре, регуляторные механизмы, подходы к балансу между инновациями и безопасностью, а также выявление общих и отличительных черт.

Цель исследования – определить ключевые тенденции в цифровом законодательстве зарубежных стран, выявить их сильные и слабые стороны, а также сформулировать рекомендации для совершенствования российской правовой системы.

Исследование базируется на сравнительно-правовом методе, системном анализе законодательных текстов и стратегических документов. В работе использованы методы классификации (группировка стран по региональному признаку), синтеза (выявление общих черт) и критического анализа (оценка противоречий).

Италия

В Италии в 2005 году принят свой аналог Цифрового кодекса, или Кодекс цифрового управления Италии [Codice Amministrazione Digitale 2005] (далее – КЦУ).

КЦУ регулирует вопросы, связанные с цифровизацией государственного управления, использованием информационных технологий в публичной администрации, а также взаимодействием между государственными органами, гражданами и частными лицами в цифровой среде. В явном виде предмет регулирования не сформулирован в виде отдельного определения, но он вытекает из содержания статей КЦУ, которые охватывают широкий спектр вопросов, связанных с цифровизацией государственного управления.

Метод регулирования КЦУ основан на принципах цифровой трансформации (эффективность, прозрачность, доступность, экономичность, безопасность и защита данных). Он не определен явно, но его содержание можно уяснить из толкования статей, которые устанавливают как обязательные нормы, так и рекомендации для государственных органов и частных лиц.

КЦУ также предусматривает разработку технических правил (Linee guida) для реализации положений кодекса, которые принимаются Агентством по цифровой Италии (AgID). Государственным органам корреспондированы обязательства по внедрению цифровых технологий, обеспечению доступа к данным и услугам в электронной форме. Кроме того, КЦУ гарантирует право граждан и предприятий на использование цифровых технологий в отношениях с государственными органами.

Необходимо отметить неоднозначность в определении некоторых терминов в КЦУ: например, термины «документо информатико» (documento informatico) и «электронная подпись» (firma elettronica) в зависимости от контекста могут трактоваться по-разному, что может привести к коллизиям при правоприменении.

КЦУ предусматривает разработку технических правил (Linee guida), но не указывает, как эти правила будут применяться на практике.

При всей лаконичности (КЦУ содержит немногим более 40 страниц текста), всё же авторам не удалось детализировать все процедуры. Ряд статей закона содержат слишком общие формулировки, что на практике может привести к различным интерпретациям и сложностям в реализации.

Для обеспечения соблюдения норм КЦУ необходимо создать механизмы контроля и мониторинга, которые будут отслеживать выполнение обязательств государственными органами и частными лицами. Кроме того, следует рассмотреть возможность упрощения процедур доступа к данным, особенно в отношении персональных данных, чтобы обеспечить баланс между защитой конфиденциальности и возможностью их повторного использования.

Таким образом, хотя рассмотренный нами КЦУ и представляет собой комплексный документ, направленный на цифровизацию государственного управления, всё же нельзя сказать, что в Италии в полной мере состоялась кодификация законодательства в цифровой сфере. Представляется, что КЦУ на сегодняшний день выступает как базовый закон в этой области, который еще требует значительной доработки в части

уточнения терминологии, детализации технических стандартов и создания механизмов контроля для устранения существующих противоречий.

Франция

Во Франции в 2016 году принят «Закон о цифровой Республике», регулирующий различные аспекты цифровых отношений в стране (далее – ЗЦР). Основным предмет регулирования включает:

- циркуляцию данных и знаний (Titre I: la circulation des données et du savoir);
- защиту прав в цифровом обществе (Titre II: la protection des droits dans la société numérique);
- доступ к цифровым технологиям (Titre III: l'accès au numérique);
- экономику данных, открытость доступа к публичным данным, защиту персональных данных, нейтральность интернета, портативность данных, регулирование платформ и другие аспекты цифровой среды [Loi n° 2016-1321 ... 2016].

Таким образом, можно констатировать, что предмет регулирования в ЗЦР достаточно полно определен и охватывает широкий спектр вопросов, связанных с цифровой экономикой, защитой данных и доступом к цифровым технологиям.

В ЗЦР устанавливаются обязательные правила и требования для администраций, операторов связи, платформ и других участников цифровой среды. Он также предусматривает создание комиссий, специальных регулирующих органов (например, Commission nationale de l'informatique et des libertés), которые контролируют выполнение норм закона. Для этого предусмотрены штрафы и другие меры наказания за несоблюдение установленных правил. Кроме того, ЗЦР поощряет использование открытых стандартов, свободного программного обеспечения и форматов.

По сути, используемый французским законодателем метод регулирования сочетает в себе законодательные, административные и стимулирующие меры, направленные на обеспечение соблюдения норм и развитие цифровой среды.

В документе закрепляется принцип нейтральности интернета, однако одновременно с этим вводятся правила, которые могут ограничивать свободу платформ в управлении контентом (например, статьи о лояльности платформ и информации для потребителей).

Общий вывод, который можно сделать при анализе этого законодательного акта, состоит в том, что он содержит внутренние противоречия, связанные с балансом между открытостью данных и их защитой, а также между свободой платформ и их регулированием.

Для преодоления этих противоречий, на наш взгляд, было бы уместно разработать однозначные критерии и механизмы, которые позволят соблюдать сбалансированный закон. Например, можно ввести дифференцированный подход к доступу к данным в зависимости от их типа и уровня конфиденциальности.

ЗЦР представляет собой базовый закон, регулирующий различные аспекты цифровой среды Франции. Он четко определяет предмет регулирования, но содержит внутренние противоречия, связанные с балансом между открытостью данных и их защитой, а также между свободой платформ и их регулированием.

Германия

В Германии также действует базовый закон – закон о цифровом правительстве [Gesetz zur Förderung der elektronischen Verwaltung 2009] (далее – ЗЦП). Он регулирует публично-правовую административную деятельность федеральных органов власти, органов земель, общин и других юридических лиц публичного права при исполнении федерального законодательства, а также судебных и правоохранительных органов, но только в той части, которая подлежит административному контролю.

К основным вопросам, которые призван урегулировать закон, относятся:

- электронный доступ к услугам (соответствующие документы, платежи, формы);
- электронная идентификация (eID, Bürgerkonto);
- цифровизация процессов (электронные акты, автоматизация обмена данными);

- открытые данные (публикация машиночитаемых данных, GovData);
- стандартизация и безопасность ИТ-систем.

В самом же законе установлены ограничения – прямо указано, на какие сферы жизни он не распространяется. В их число входят: уголовное преследование, налоговые расследования, социальное обеспечение, а также деятельность патентных ведомств и судебные процедуры.

ЗЦП вводит централизованные инструменты, которыми обязывает в своей повседневной деятельности пользоваться органы власти: учреждает административный портал федерации (§ 9a), центральную службу электронных печатей (§ 2a), а также национальный портал метаданных (GovData), § 12a.

В соответствии с предписаниями ЗЦП, органы власти обязаны предоставлять государственные услуги в электронном виде (например, путем обеспечения доступа к материалам о своей деятельности (§ 2), ведения электронных счетов (§ 4a), использования электронных подписей и печатей (§ 2a), а также внедрения электронного делопроизводства (§ 6a, § 7)).

Координацией этой деятельности занимается IT-Planungsrat – совет по ИТ-планированию, который является центральным органом, руководящим цифровизацией государственного управления в Германии. Состоит из 17 членов, в число которых входят представители федерального правительства и правительств земель. Представители местных органов власти участвуют в заседаниях с правом совещательного голоса.

Руководит на федеральном уровне IT-Rat (§ 10) – Федеральный совет по ИТ, который устанавливает стратегические руководящие принципы и принимает обязательные решения в рамках межведомственного взаимодействия.

Хотя ЗЦП зачастую только содержит указание на необходимость разработки подзаконных актов, некоторые из них прямо упомянуты, например правила электронного счетоводства (§ 4a(3)). ЗЦП также устанавливает механизм контроля, который включает в себя отчетность перед Бундестагом (§ 12a(11)) и дальнейшую оценку реализации (§ 6(2)).

Поскольку ЗЦП, по сути, представляет собой рамочный закон, в нем не учтен ряд нюансов. В частности, муниципалитеты и общины могут не иметь достаточных технических и финансовых ресурсов для реализации тех полномочий, которые на них возложены законом (§ 1(4), § 4(4)), однако ЗЦП не проясняет, как в таком случае должен выглядеть бюджетный процесс.

При этом остается открытым вопрос возможных коллизий между федеральными и земельными законами, особенно при регулировании открытых данных (§ 12a(5)), поскольку оно отнесено к вопросам совместного ведения.

Хотя в ЗЦП встречается такое понятие, как долгосрочное хранение электронных документов (§ 7(1)), четких требований к нему не содержится. Есть также и определенные неясности в правилах автоматизированного обмена данными между государственными органами (§ 5, § 5a), особенно при трансграничных запросах (§ 5a(3)), что неизбежно влечет за собой риски нарушения защиты данных.

Резюмируя общую характеристику ЗЦП, необходимо отметить, что он создает правовую основу для цифровизации госуправления, но эффективность его реализации во многом зависит от устранения ресурсных и технических барьеров, коллизий федерального и земельного законодательства, что, в свою очередь, неизбежно требует четкой регламентации защиты данных и исчерпывающего перечня исключений.

Великобритания

В Соединенном Королевстве в 2017 году принят, возможно, один самых обстоятельных базовых законов о цифровизации. Закон о цифровой экономике [Digital Economy Act 2017] (далее – ЗЦЭ), подробно и детально описывает практически все аспекты общественных отношений, связанные с внедрением цифровых технологий.

Круг регулируемых отношений довольно широк. В частности, он включает вопросы «цифрового правительства», описывает обмен данными между госорганами для улуч-

шения качества услуг (например, по вопросам борьбы с недостаточным обеспечением энергоресурсами, управления долгами, предотвращения мошенничеств), поддержки исследований. ЗЦЭ содержит требования к раскрытию информации государственными органами (Часть 5, глава 7).

ЗЦЭ также регулирует порядок сбора и использования данных, порядок взаимодействия с Office for National Statistics (ONS) – Национальным статистическим управлением, устанавливает порядок раскрытия неидентифицирующей информации для общественных целей.

ЗЦЭ детально описывает вопросы построения и содержания цифровой инфраструктуры в стране. Например, для обеспечения полноценного доступа граждан к получению цифровых услуг минимальная скорость широкополосного интернета должна составлять 10 Мбит/с (с возможностью повышения до 30 Мбит/с), для потребителей предусмотрена автоматическая компенсация за нарушение стандартов качества.

Основным регулятором государственной политики в этой сфере является OFCOM (Office of Communications), который контролирует соблюдение требований к телекоммуникациям, радиочастотному спектру и защите пользователей.

На OFCOM возложена обязанность также контролировать соблюдение стандартов вещания, прав пользователей. Для этого регулятору делегированы полномочия (подотчетность операторов связи, регулирование инфраструктуры, лицензирование BBC) (Часть 6 закона).

Часть функций реализует ICO (Information Commissioner's Office) – офис «комиссара по информации», который обеспечивает соблюдение правил обработки данных.

Службы налогов и сборов, в том числе центральная HMRC, а также служба Уэльса Welsh Revenue Authority и Шотландии Revenue Scotland в рамках этого закона наделены полномочиями по регулированию раскрытия налоговой информации.

ЗЦЭ ужесточает ответственность за нарушение авторских прав, регулирует использование электронных книг в публичных библиотеках, подробно описывает защиту прав потребителей, в частности разрешает установку лимитов на расходы в мобильной связи, защиту от вторичной продажи билетов, приобретенных в онлайн-кассах.

Однако даже при такой степени детализации процессов цифровизации ЗЦЭ не избежал ряда недостатков, в основном связанных с расплывчатыми формулировками и пробелами правового регулирования.

В частности, в законе использованы в качестве общеупотребительных понятия «общественный интерес», «антисоциальное поведение», «разумность» действий, ими предлагается руководствоваться уполномоченным органам при раскрытии неидентифицируемой информации (Часть 6) или при удалении оборудования. Неоднозначная, субъективная трактовка этих понятий может вызывать разночтения и, соответственно, разнонаправленное правоприменение.

Хотя закон был принят в 2017 году, в нем отсутствуют четкие правила для современных платформ, уже существовавших на то время (например, стриминговых сервисов).

Как итог ЗЦЭ создает детальную правовую базу для развития цифровой инфраструктуры, но его сложность и обширность требуют дополнительных разъяснений и подзаконных актов. Закон балансирует между интересами операторов и собственников, однако пробелы в формулировках и процедурные барьеры могут стать источниками споров.

Закон требует доработки в части детализации процедур и учета современных технологических вызовов. Предусмотренные санкции обеспечивают соблюдение требований, однако избыточная бюрократия и неоднозначные формулировки могут осложнить применение закона.

Соединенные Штаты Америки

В США в 2002 году принят закон об электронном правительстве [E-Government Act ... 2002] (далее – ЗЭП). Круг регулируемых отношений определен в самом законе и носит исчерпывающий характер.

Общее управление электронным правительством осуществляет вновь созданная структура – на федеральном уровне это СЮ (Управление электронного правительства) в составе ОМВ (Административно-бюджетного управления администрации президента), которое призвано координировать ИТ-стратегии всех федеральных агентств. Описаны процедуры межведомственного взаимодействия. В частности, ключевые статистические агентства – Бюро переписи, Бюро экономического анализа, Бюро трудовой статистики – должны проводить обмен данными между собой для повышения эффективности. Кроме того, федеральные ведомства должны предусмотреть программы развития ИТ-навыков госслужащих.

ЗЭП содержит требования к защите данных, включая стандарты безопасности и оценку рисков. Ряд положений посвящен повышению доступности государственных услуг, в том числе развитию интернет-порталов для граждан, переводу информации в цифровой формат. ЗЭП определяет ключевой принцип конфиденциальности данных, устанавливая, что сбор персональной информации и использование данных возможны только для статистических целей.

Для реализации этих задач ЗЭП предусматривает ряд организационных и правовых механизмов. В частности, СЮ координирует другие федеральные ведомства посредством их участия в Совете директоров по информационным технологиям, в который входят соответствующие руководители всех министерств и агентств (CIO Council). СЮ обязан периодически отчитываться не только перед ОМВ в администрации президента, но и перед Конгрессом США. Создан специальный фонд (E-Government Fund) для финансирования инновационных проектов.

ЗЭП предусматривает введение обязательных стандартов информационной безопасности и указывает на структуру, ответственную за их разработку – NIST (Национальный институт стандартов и технологий США), подразделение Управления по технологиям США, которое является одним из агентств Министерства торговли США.

На проекты, которые не соответствуют этим требованиям, не прошли независимый аудит информационных систем (включая оценку уязвимостей), налагается ряд финансовых ограничений.

За незаконное разглашение конфиденциальных данных вводится уголовная ответственность (с максимальной санкцией до 5 лет тюрьмы и различные штрафы).

Хотя ЗЭП с очевидностью носит рамочный характер и был принят по меркам информационных технологий достаточно давно, нельзя не отметить некоторые недостатки, пробелы и противоречия, которые в нем содержатся, несмотря на все поздние поправки.

Неясно, в частности, как сочетаются требования к открытой публикации данных по закону FOIA (Freedom of Information Act), закону о свободе информации с требованиями о защите персональных данных (например, в контексте сбора для целей государственной статистики). Несмотря на то что в ЗЭП явно сделан акцент на безопасности, он не предусматривает механизмов быстрого реагирования на новые виды кибератак.

Некоторые положения (например, обмен данными) распространяются только на три статистических агентства, такой ограниченный охват сужает потенциальную эффективность, при этом существующие различия в ИТ-инфраструктуре и стандартах между другими агентствами могут существенно замедлить интеграцию технических решений и оказание государственных услуг.

Интересно, что ОМВ через CIO Council получает неожиданно широкие полномочия по контролю всех федеральных ведомств, что создает избыточные коррупционные риски. Также сохраняется риск использования данных, собранных для статистики, в административных целях, несмотря на установленные запреты.

Реализация многих инициатив, описанных в ЗЭП, требует значительных бюджетных вливаний на протяжении многих лет, что в долгосрочной перспективе неизбежно создает риск недофинансирования.

Резюмируя анализ основных положений ЗЭП, отметим, что в целом закон заложил основу для цифровизации государственных услуг и повышения безопасности данных, но его эффективность зависит от ресурсного обеспечения, межведомственной координации и адаптации к быстро меняющимся технологическим вызовам. Проблемы финансирования, кибербезопасности и баланса между открытостью и конфиденциальностью остаются ключевыми вызовами.

Китай

Цифровое законодательство Китая разнообразно и состоит из многочисленных отдельных законодательных актов. В этой сфере в КНР действуют следующие специальные законы: об электронной торговле, об электронной подписи, о кибербезопасности, о безопасности КНР, о защите личной информации и закон о безопасности данных. Кодификация в строгом смысле этого слова в отношении цифрового законодательства в Китае не проводилась, однако обобщение путем консолидации все же осуществлено.

В Китае был опубликован официальный сборник Госсовета КНР «Совместное создание сообщества единой судьбы в киберпространстве» в ноябре 2022 года в формате White Paper (Белая книга) – всеобъемлющий документ, в котором изложен подход страны к регулированию цифровой среды [White Paper on Cyber Law 2022] (далее – БК).

БК охватывает комплексное регулирование цифрового пространства Китая, включая регулирование сбора, хранения, трансграничной передачи данных, защиту персональной информации, обеспечение безопасности критической информационной инфраструктуры, регулирование алгоритмов, управление контентом, регулирование ИИ, алгоритмов, автономного транспорта, блокчейна. Отдельный раздел посвящен международному взаимодействию, в том числе адаптации к глобальным трендам (например, совместимости стандартов трансграничных данных, сотрудничеству с ЕС).

В БК указаны многочисленные контрольные механизмы, призванные приводить в исполнение государственную политику в цифровом пространстве.

Введены процедуры лицензирования и сертификация, причем не только в отношении интернет-сервисов и платформ, но и в отношении алгоритмов (например, предусматривается регистрация алгоритмов с «общественным влиянием»).

Введен надзор за платформами – установлен запрет на монополистические практики, установлены ограничения для крупных платформ (например, широко известных и популярных Tencent, Alibaba).

Проводится обязательная проверка трансграничных передач данных, введены технические стандарты, действие которых охватывает практически все новейшие явления цифровой среды: регулирование ИИ, 5G, автономных автомобилей.

За нарушения в сфере киберзаконодательства предусмотрены обширные санкции, в том числе: административные наказания (штрафы за нарушения в области защиты данных до 5 % оборота компании), уголовная ответственность за распространение «ложной информации», кибератаки, утечки данных (до 15 лет лишения свободы по закону о военной дезинформации).

Для платформ и сервисов возможна блокировка (например, приостановка деятельности за недостоверный контент), запреты (ограничение доступа иностранных технологий (например, для Huawei в 5G-сетях)).

При анализе БК обращает на себя внимание жесткий, возможно даже избыточный контроль, который осуществляют государственные органы практически над всеми явлениями цифровой среды. Представляется, что очень строгие требования к данным и алгоритмам в итоге могут замедлить инновации, а описанные ограничения на трансграничную передачу данных усложнить развитие международного бизнеса.

При этом парадоксально, что фактически быстрое развитие ИИ, метавселенных опережает даже такое прогрессивное законодательство, поскольку оно содержит пробелы в регулировании новейших технологий. Неясно, например, как урегулирован правовой статус NFT, какой набор данных необходим для определения «цифровых идентичностей» и каков уровень их правовой защиты.

В БК усматривается также институциональное противоречие между защитой данных (например, в нормах, подобных европейскому регламенту GDPR) и интересами национальной безопасности (например, при обеспечении доступа к данным спецслужб). При этом применяются неоправданно широкие формулировки (например, понятие «угроза национальной безопасности» в БК не расшифровано). Процесс принятия решений, утверждения стандартов и санкций непрозрачен, что в целом создает коррупционные риски произвольного усмотрения правоприменителя.

В отличие от ряда стран, рассмотренных нами выше, цифровое законодательство Китая носит подробный, всеобъемлющий характер. БК отражает стремление национального законодателя создать такую систему, которая сочетала бы безопасность, контроль и технологическое развитие. Однако избыточная регуляторная нагрузка и быстрое развитие технологий создают вызовы для баланса между инновациями, правами граждан и интересами государства.

Индия

В Индии в 2023 году принят DIA, «закон о цифровой Индии» (далее – ЗЦИ). Он заменил собой устаревший Акт об информационных технологиях 2000 года, который регулировал весьма ограниченный круг вопросов, таких как юридическое признание электронных записей, транзакций и подписей. Новый ЗЦИ охватывает широкий спектр цифровых отношений, включая электронную коммерцию, социальные медиа, безопасность пользователей, защиту прав пользователей, борьбу с дезинформацией, радикализацией, недобросовестной торговой практикой [Chauriha 2023]. ЗЦИ также регулирует новейшие явления цифровой среды, такие как блокчейн и искусственный интеллект.

Важной новацией в нем является пересмотр подхода к принципу «safe harbor» (безопасной гавани), согласно которому цифровые платформы ранее не несли ответственности за контент пользователей. Теперь платформы лишены такого иммунитета и обязаны соблюдать строгие стандарты отчетности. Можно спрогнозировать, что это может привести к излишней осторожности платформ при модерации контента и в конечном итоге к ограничению свободы выражения мнений. Кроме того, введено требование KYC (англ. «Know Your Customer» – знай своего клиента) для носимых устройств, что усиливает контроль за пользователями.

Общий анализ ЗЦИ позволяет сделать вывод, что содержащиеся в нем требования внутренне противоречивы, поскольку имеют разнонаправленные цели.

Одновременно защищать права граждан и учитывать интересы технологических компаний сложно, что создает риск потенциальных конфликтов. Строгие нормы (например, специализированный механизм для рассмотрения гражданских и уголовных правонарушений в интернете) могут замедлить развитие стартапов и отпугнуть иностранные инвестиции, особенно в сфере новых технологий.

Для эффективного исполнения закона потребуются значительные ресурсы, экспертиза и инфраструктура. В целом же ЗЦИ представляет собой позитивный шаг в регулировании цифровой среды, однако его реализация сопряжена с рядом вызовов, включая баланс между инновациями и безопасностью, а также обеспечение эффективного исполнения. Успех закона будет зависеть от его адаптации к динамично меняющемуся цифровому ландшафту.

Сингапур

Республика Сингапур – один из «ветеранов» цифрового законодательства. Различные нормативные акты в этой сфере принимаются в стране с 1980-х годов, но они не объединяются в какой-либо кодекс. Сопряжение законодательства в цифровой сфере и его согласованная работа обеспечиваются путем принятия государственных программ, действующих на определенные периоды.

В настоящее время в стране работает iN2015 (Intelligent Nation 2015) – генеральный план, рассчитанный до 2025 года [iN2015 Masterplan 2015]. Его реализацию координирует Управление по развитию инфокоммуникационных медиа (IMDA) при Министерстве цифрового развития и информации (MDDI) Сингапура.

План iN2015 охватывает практически все сферы жизни, детально и подробно описывает регулирование общественных отношений, описывает цифровую трансформацию государственного сектора Сингапура.

Предусматривается еще большая цифровизация государственных услуг, и без того находящаяся на высоком уровне, она коснется транзакций для граждан и бизнеса (процессы LifeSG, GoBusiness), автоматизации судебного делопроизводства (например, проверка судебных решений через систему Authentic Court Orders (ACO)).

Для реализации программы установлены соответствующие KPI (например, проведение 90–95 % транзакций в цифровом виде, 100 % е-платежей), облачная миграция систем (70 % к 2023 г.)

Программа предусматривает внедрение AI, IoT, блокчейна (OpenCerts), облачных решений работу общих (CODEX, SGTS) и специальных (SCOPE, Developer Portal) цифровых платформ для населения, бизнеса, научного сообщества.

Отдельный раздел посвящен развитию цифровой грамотности (Digital Clinics), обучению госслужащих (20 тысяч обученных к 2023 г.), создание Центра передового опыта (CentEx). Программа также предусматривает поддержку уязвимых групп населения при адаптации к технологиям цифровой среды (GALE, eCanvas). Предусмотрены подпрограммы обучения (Data Science, Digital Academy), в том числе лидерские (Smart Nation Scholarship).

Необходимо отметить, что в области укрепления кибербезопасности и защиты данных упор сделан на требования Public Sector Governance Act 2018 года, однако ряд норм этого документа уже непригоден, так как недостаточно детализирует меры противодействия сложным угрозам.

Оценивая программу в целом, стоит отметить, что ее реализация требует значительных ресурсов и длительной координации всех привлеченных служб. При этом сохраняются технологические риски, такие как зависимость от инноваций (блокчейн, AI) без четких планов на случай их неэффективности. Также неясно, как будут корректироваться KPI при изменении технологического ландшафта.

План iN2015 внушает осторожный оптимизм тем, что до сих пор в Сингапуре такие программы являлись примерами успеха для всех заинтересованных стран – ранее реализованные проекты вроде TraceTogether, MyInfo укрепляют доверие к государственной политике в этом вопросе.

Кроме того, план один из немногих, который не только учитывает развитие информационных технологий, но и удачно сочетает это с адаптацией к условиям жизни в период пост-COVID: сделан акцент на удаленной работе, цифровых решениях в кризисных ситуациях (например, контактная трассировка). Таким образом, цифровизация используется для экономического восстановления и устойчивого развития страны.

Как итог – документ представляет собой амбициозную комплексную стратегию, сочетающую технологические инновации, обучение и партнерства. Однако успех его реализации во многом зависит от преодоления ресурсных ограничений, усиления мер безопасности и обеспечения инклюзивности.

Заключение

В процессе сравнительного анализа цифрового законодательства нам удалось выделить как общие, так и специфические особенности, свойственные законодотворчеству рассмотренных стран.

Страны западного блока (Италия, Франция, Великобритания, США) демонстрируют следующие общие характеристики:

1. Акцент на цифровизации госуправления. Все изученные законы направлены на переход к электронным услугам, включая электронные подписи, документооборот и автоматизацию процессов.

2. Баланс между открытостью данных и их защитой: законы стремятся обеспечить прозрачность (публикация открытых данных) при соблюдении конфиденциальности.

3. Введение особых регуляторных механизмов. В рассмотренных странах созданы специализированные органы (OFCOM в Великобритании, AgID в Италии) и предусмотрены санкции за нарушения (от административных штрафов до уголовной ответственности).

4. Акцент на соблюдении прав граждан: гарантируется доступ к цифровым технологиям и защита прав пользователей.

Азиатские страны (Китай, Индия, Сингапур) объединяют следующие особенности:

1. Акцент на национальной безопасности и борьбе с дезинформацией. Предусмотрен жесткий контроль данных и контента.

2. Централизованное управление технологиями. Регулирование новейших технологий (ИИ, блокчейн) осуществляется через такие процедуры, как лицензирование и сертификация.

3. Развитие цифровой среды происходит преимущественно через механизм государственно-частного партнерства.

4. Акцент на приоритете национальных интересов. Например, практикуется ограничение иностранных технологий (Китай) и поддержка локальных инноваций (Индия).

Таким образом, западные страны делают акцент на правах граждан, балансе между открытостью и приватностью, тогда как азиатские – на контроле, безопасности и суверенитете. В западных законах преобладают децентрализованные механизмы регулирования, а в азиатских – централизованные и иерархические. В первой группе выше толерантность к инновациям, во второй – стремление к технологическому лидерству через жесткое регулирование.

Можно выделить также и общие черты, объединяющие все рассмотренные законы.

1. Цифровизация госуслуг. Все страны так или иначе стремятся к автоматизации и доступности услуг (например, внедрение электронных порталов в США, LifeSG в Сингапуре).

2. Кибербезопасность. Включение мер защиты данных и инфраструктуры разной степени жесткости также отмечено во всех нормативных актах (NIST в США, Public Sector Governance Act в Сингапуре).

3. Во всех рассмотренных случаях неизбежно присутствуют риски реализации: ресурсные ограничения, бюрократия, пробелы в регулировании новых технологий.

Общее преимущество цифрового законодательства стран Азии и Западной Европы состоит, очевидно, в повышении эффективности госуправления, большой прозрачности государственных процедур, обеспечении защиты прав пользователей. Общий недостаток во всех случаях также очевиден – это риск избыточного регулирования, конфликты между инновациями и безопасностью, сложности межведомственной координации.

Представляется, что Россия могла бы почерпнуть многое для себя из лучших зарубежных практик. В частности, из опыта западных стран стоило бы обратить внимание на внедрение электронных услуг с акцентом на соблюдении прав граждан (например, аналоги eID), развитии открытых данных при сохранении конфиденциальности. В опыте азиатских стран в первую очередь обращают на себя внимание создание централизованных регуляторных органов для кибербезопасности, поддержка локальных технологических решений.

Универсальными мерами, которые одинаково положительно можно оценить в каждом из рассмотренных случаев, можно считать инвестиции в инфраструктуру и обучение госслужащих, гибкое регулирование, адаптируемое к технологическим изменениям, соблюдение баланса между контролем и свободой инноваций в цифровой среде.

Как итог, на наш взгляд, стратегия России в области развития цифрового законодательства должна сочетать лучшие практики: прозрачность и права граждан по западной модели, а также системный подход к безопасности и технологическому суверени-

тету – по азиатской. Ключевой задачей остается минимизация бюрократии и создание условий для устойчивой цифровой трансформации.

Список источников

- Модельный Информационный кодекс для государств – участников СНГ (новая редакция) (принят на 54-м пленарном заседании Межпарламентской Ассамблеи государств – участников СНГ, Постановление № 54-12 от 28.10.2022) // Гарант : информационно-правовой портал. 2022. URL: <https://base.garant.ru/406327849/53f89421bbdaf741eb2d1ecc4ddb4c33/> (дата обращения: 27.03.2025).
- Цифровой кодекс Кыргызской Республики // Жогорку Кенеш : официальный сайт парламента Кыргызской Республики. 12.12.2024. URL: <https://kenesh.kg/law-activity/movements/5511> (дата обращения: 27.03.2025).
- Chauriha S. Explained: The Digital India Act 2023 // Vidhi Legal Policy : website. 08.08.2023. URL: <https://vidhilegalpolicy.in/blog/explained-the-digital-india-act-2023/> (access date: 27.03.2025).
- Codice Amministrazione Digitale // L'Agenzia per l'Italia Digitale. Roma, 2005. URL: <https://www.agid.gov.it/it/agenzia/strategia-quadro-normativo/codice-amministrazione-digitale> (access date: 27.03.2025).
- Digital Economy Act 2017 // The National Archives : official website. URL: <https://www.legislation.gov.uk/ukpga/2017/30/contents> (access date: 27.03.2025).
- E-Government Act of 2002 // U.S. Department of Justice. Office of Privacy and Civil Liberties : official website. Washington, 2002. URL: <https://www.justice.gov/opcl/e-government-act-2002> (access date: 27.03.2025).
- Gesetz zur Förderung der elektronischen Verwaltung (EGovernment-Gesetz - EGovG) // Das Bundesministerium der Justiz. 2009. URL: <https://www.gesetze-im-internet.de/egovg/> (access date: 27.03.2025).
- In2015 Masterplan. Infocomm Development Authority of Singapore, 2015. URL: <https://web.archive.org/web/20121109064438/http://www.ida.gov.sg/Infocomm-Landscape/iN2015-Masterplan.aspx> (access date: 27.03.2025).
- Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique // Journal Officiel de la République Française. 2016. 8 octobre. URL: <https://www.wipo.int/wipolex/ru/legislation/details/16380> (access date: 27.03.2025).
- White Paper on Cyber Law // China Academy of Information and Communications Technology : official website. 2022. URL: <https://www.caict.ac.cn/english/research/whitepapers/index.html> (access date: 27.03.2025).

Информация об авторе

Анатолий Борисович Чиквин, аспирант, Уральский институт управления Российской академии народного хозяйства и государственной службы при Президенте РФ, Екатеринбург, Россия

Information about the author

Anatolii B. Chikvin, a postgraduate student, Ural Institute of Management, Russian Academy of National Economy and Public Administration under the President of the Russian Federation (Yekaterinburg, Russia).

Статья поступила в редакцию | Submitted 31.03.2025.

Одобрена после рецензирования | Revised 22.04.2025.

Принята к публикации | Accepted 22.04.2025.