GRATA INTERNATIONAL

Цифровой комплаенс-2026:

коллизии Цифрового Кодекса, законодательства об искусственном интеллекте и персональных данных в РК

Сауле Ахметова

Партнер,
GRATA International
Казахстан, Алматы

2026

Цифровой комплаенс-2026: коллизии Цифрового Кодекса, законодательства об искусственном интеллекте и персональных данных в РК

За последние месяцы цифровое законодательство Казахстана пережило полную перезагрузку. Январский «запуск» Закона РК «Об искусственном интеллекте» (Закон «Об ИИ»), поправки в Закон РК «О персональных данных и их защите» (Закон «О персональных данных») и масштабная кодификация отрасли в виде Цифрового Кодекса РК изменили правила игры.

Анализ новой регуляторной базы выявил системную несогласованность некоторых норм. Пытаясь объять необъятное, законодатель оставил некоторые «серые зоны» в правовом регулировании. Ниже описываются, некоторые положения законов, которые создают риски для бизнеса.

1. Рекомендательные системы: проблемы классификации и ловушка автономности

Анализ положений нового законодательства выявил методологический разрыв, который ставит под удар контентные и торговые платформы (маркетплейсы, интернет-магазины, медиаресурсы). Проблема кроется в имплементации относительно того, как Закон «Об ИИ» классифицирует алгоритмы.

Владельцы платформ могут относить свои рекомендательные ленты (умные подборки товаров или новостей) к системам низкой автономности (пункт 2 статьи 17 Закона «Об ИИ»). Бизнес может понимать это таким

образом, что алгоритм лишь формирует варианты, а финальное действие — клик по карточке или покупка — всегда остается за конечным потребителем. Опираясь на эту логику, компании полагают, что находятся в безопасности: ведь жесткие запреты пункта 3 статьи 17 (включая табу на скрытый профайлинг и манипулирование подсознанием) направлены в первую очередь на системы высокой автономности.

Однако такой подход содержит фундаментальную юридическую ошибку. Определяя системы низкой автономности как те, где «окончательный выбор и действия всегда осуществляются человеком», законодатель опирается на международную концепцию контроля (human-in-the-loop). В этой конструкции «человек» — это не конечный потребитель, реагирующий на рекламу, а оператор на стороне владельца ИИ-системы.

Действие рекомендательного алгоритма заключается не в покупке товара, а в его алгоритмическом отборе и показе. Поскольку умная лента маркетплейса формируется и выводится на экран пользователя за миллисекунды в режиме реального времени, ни один сотрудник компании не способен осуществить предварительную проверку и одобрение каждого показа. Это означает, что система принимает решение и действует автономно.

Следствием этой правовой иллюзии становится то, что при первой же проверке регулятор (Министерство ИИ и цифрового развития РК) может переквалифицировать безобидную, по мнению бизнеса, рекомендательную систему в систему средней или высокой автономности. Как только это произойдет, на обычную персонализированную выдачу товаров обрушатся жесткие запреты Закона «Об ИИ». Любая попытка алгоритма удержать внимание пользователя за счет скрытой подстройки под его поведенческие слабости может быть квалифицирована не как «эффективный маркетинг», а как незаконное манипулирование, эксплуатирующее уязвимости потребителя.

Чтобы избежать ответственности за неверную классификацию систем, бизнесу необходимо пересмотреть архитектуру рекомендательных сервисов. Если компания не может обеспечить ручной контроль каждого действия ИИ, ей придется внедрить превентивные интерфейсные ограничения. Пользователю должна быть предоставлена понятная

техническая возможность в один клик полностью отключить поведенческую (автономную) персонализацию, переведя ленту в режим простой хронологической выдачи. Это станет главным аргументом того, что платформа не применяет к клиенту автономные манипулятивные практики.

2. Цифровой маркетинг и средняя автономность: парадокс мгновенных решений и неисполнимое право на информирование

Другой методологический тупик возникает в сфере автоматизированного размещения интернет-рекламы. Интеллектуальные маркетинговые платформы подпадают под категорию систем средней автономности (пункт 2 статьи 17 Закона «Об ИИ»). В отличие от иллюзии «низкой автономности», здесь бизнес и закон признают очевидное: алгоритм самостоятельно и мгновенно принимает микрорешения о том, какому именно пользователю показать объявление. При этом система остается в правовом поле средней автономности только потому, что человек-оператор (маркетолог) осуществляет верхнеуровневый контроль — он задает бюджет, границы таргетинга и может в любой момент отменить всю рекламную кампанию.

Однако, успешно квалифицировав свои системы и избежав абсолютных запретов на высокую автономию (пункт 3 статьи 17 Закона «Об ИИ»), маркетологи попадают в тиски другой нормы — фундаментального принципа прозрачности и объяснимости для любых ИИ-систем (статья 7 Закона «Об ИИ»), предусматривающей право пользователя на информацию о характеристиках и ограничениях системы ИИ, о порядке автоматизированной обработки и ее последствиях.

Комплаенс-риск и пробел регулирования скрываются на стыке технологий и этого общего принципа права, обнажая парадокс мгновенной автоматизации. Развертывание таргетированной рекламы — это процесс, в ходе которого ИИ за миллисекунды принимает решение (выделить конкретного потребителя из тысяч и показать ему баннер), которое ведет к определенным последствиям (изменению его потребительского поведения). Физически невозможно в это же самое мгновение предоставить человеку полную информацию о логике обработки его профиля и последствиях показа, как того императивно требует статья 7 Закона «Об ИИ».

Из-за того, что закон не детализирует регулирование п данному вопросу для различных систем ИИ, возникает непреодолимый тупик: технология технически не способна выполнить общую норму о прозрачности в режиме реального времени. Проверка регулятора постфактум может интерпретировать отсутствие моментального раскрытия логики показа баннера как нарушение прав пользователя. В условиях общих положений статьи 7 Закона «Об ИИ» сфера цифрового маркетинга в Казахстане перемещается в зону комплаенс-риска.

Чтобы защитить бизнес от нарушений закона из-за слишком быстрой и автоматизированной интернет-рекламы, компаниям необходимо действовать на опережение, переведя абстрактные юридические правила в плоскость интерфейсных решений. Прежде всего, стоит отказаться от работы со сторонними ИИ-сервисами («черными ящиками»), если их разработчики не способны внятно объяснить логику работы своих алгоритмов таргетинга. При этом вместо сложных многостраничных юридических документов на сайте или в мобильном приложении рекомендуется внедрить простое и наглядное окно приветствия. В нем нужно доступным языком заранее раскрыть пользователю порядок работы ИИ: объяснить, что система будет анализировать его просмотры исключительно ради подбора персональных предложений. Когда пользователь видит такое предупреждение и осознанно дает свое согласие до начала алгоритмической обработки, невыполнимое в миллисекундах требование закона о прозрачности превращается в понятный договор между компанией и ее клиентом.

3. Регуляторный шлагбаум: извлечение открытых данных на стыке бизнеса и борьбы со спамом

В отличие от предыдущих положений законов, в вопросе сбора общедоступных персональных данных законодатель не оставил бизнесу «серых зон». Пункт 11 статьи 7 Закона «О персональных данных» сформулирован как бескомпромиссный и прямой запрет: сбор и обработка персональных данных для создания или расширения любых баз данных посредством их нецелевого извлечения из общедоступных источников категорически запрещены. Эта норма ставит жесткий регуляторный

шлагбаум перед практикой формирования коммерческих списков из сети. При этом закон не делает разницы между высокими технологиями и ручным трудом: под запрет попадает любой способ извлечения информации — от автоматизированного парсинга до банального копирования контактов вручную. Масштаб этого запрета раскрывается через сложную двоякую природу правоприменения, затрагивающую как деловую среду, так и повседневную жизнь граждан.

С одной стороны, в плоскости чистых бизнес-коммуникаций регулятор потенциально может применять гибкое, ограниченное толкование права на неприкосновенность частной жизни. Когда адвокат, нотариус или независимый консультант открыто публикует свои ФИО и рабочий телефон на официальном ресурсе, эта информация носит сугубо профессиональный характер. Оценка таких сведений уполномоченным органом может смещаться в сторону «делового контекста», поскольку публикация контактов здесь является условием ведения практики. Однако даже в этом сегменте сбор контактов для внесения в сторонние коммерческие CRM-системы (неважно, силами маркетингового робота или руками менеджера по продажам) теперь формально признается нецелевым и неправомерным, если на это не было получено прямое согласие.

С другой стороны, истинная цель законодательного барьера лежит в плоскости защиты обычных граждан от агрессивного B2C-маркетинга. Открытые цифровые платформы, телефонные справочники и доски объявлений годами служили бесплатными сырьевыми базами для бизнеса. Массовое извлечение номеров и адресов электронной почты обычных физических лиц привело к расцвету навязчивого спама. Новая норма полностью ликвидировала иллюзию «ничейных данных в интернете», провозгласив: тот факт, что человек выложил свой телефон или электронный адрес в сеть (например, чтобы продать предмет мебели), не дает права сторонней компании забирать этот номер в свои базы данных для последующего прозвона и электронной коммуникации. Любое накопление таких сведений без прямого и целевого согласия субъекта персональных данных теперь является правонарушением, за которое компании грозят санкции.

Чтобы обезопасить компанию от проверок регулятора, бизнесу необходимо полностью свернуть практику сбора контактов из внешних открытых источников, прекратив как автоматический скрапинг, так и ручное формирование баз силами сотрудников. Единственным легальным путем формирования клиентской базы становится модель входящего маркетинга, когда потенциальные клиенты и партнеры самостоятельно и осознанно передают свои сведения. На практике это требует перевода коммуникаций на собственные ресурсы организации: корпоративные сайты, посадочные страницы или защищенные формы подписок. В этой модели пользователь сам, заполняя анкету или регистрируясь на вебинар, совершает целевое действие на экране, тем самым предоставляя компании законное право на обработку его данных, что исключает риски обвинений в нецелевом извлечении информации из общедоступных источников.

4. Кризис цифровой архитектуры: системная ловушка неопределенных идентификаторов для корпоративного ИТ

Новые правила создали проблему, которая выходит далеко за рамки интернет-маркетинга и затрагивает практически любые цифровые системы бизнеса — от систем лояльности ритейла до внутренних ERP-, CRM- и HR-платформ. Эта ситуация возникла из-за несогласованности норм. С одной стороны, статья 45 Цифрового кодекса вводит категорию идентификаторов цифровых данных, выделяя уникальные идентификаторы для физического и юридического лица. С другой стороны, Закон «О персональных данных» изменил определение: теперь персональными данными признаются сведения о человеке, дополненные одним или несколькими идентификаторами. В результате такое наложение норм превращает обычные технические процессы компаний в зону жесткого правового регулирования.

Главный методологический изъян и системная ловушка законодателя заключаются в том, что Закон «О персональных данных» и Цифровой Кодекс не указывают, имеет ли значение вид идентификатора для «включения» правовой защиты, и не приводят хотя бы примерный перечень таких цифровых маркеров. В результате под действие Закона теоретически может подпасть любой внутренний цифровой след: номер

дисконтной карты, внутренний User ID в базе данных, токен мобильного приложения, табельный номер сотрудника в HR-системе или ID трекера на логистическом транспорте.

В теории, взаимное применение указанных норм создает гипотетический риск того, что под надзорный периметр могут подпасть даже самые рутинные цифровые следы — например, запись о покупке товара, лог входа в здание или фиксация рабочего времени, если они привязаны к внутреннему ID. Однако утверждать это категорично было бы преждевременно. Реальная интерпретация со стороны Министерства ИИ и цифрового развития РК может пойти по совершенно иному пути. Если опираться на историческую практику отечественного регулятора, уполномоченный орган всегда узко подходил к интерпретации персональных данных, рассматривая персональной информацией только ту, которая сама по себе в изоляции от других сведений позволяла идентифицировать личность, к примеру, отмечая в одном из разъяснений, что ИИН сам по себе «в отрыве» от ФИО не относится к персональным данным. Тем не менее, отсутствие в новом определении понятия «персональные данные» четких критериев «дополняемости» данных, равно как и отсутствие в статье 45 Цифрового Кодекса перечня частных идентификаторов, создает для корпоративного сектора ситуацию предсказуемой неопределенности. Никто не может гарантировать, где именно уполномоченный орган проведет границу между технической аналитикой логов и защищаемой приватностью в ходе будущих проверок.

Чтобы минимизировать риски в условиях этой методологической двусмысленности, компаниям необходимо действовать на опережение и превентивно защищать свои технологические процессы. Логическим решением становится разумное разделение и структурирование потоков информации на уровне архитектуры баз данных. На практике это означает, что внутренние ИТ-контуры организации должны быть четко сегментированы: технические учетные записи, лог-файлы и частные идентификаторы систем автоматизации должны обрабатываться изолированно от содержательных, анкетных сведений о клиентах или сотрудниках. Любое их взаимное слияние или «дополнение», в результате которого технический лог жестко связывается с реальным профилем лица,

должно быть прозрачным и юридически обоснованным внутри внутренних политик компании. Такой сбалансированный подход позволит застраховать бизнес от непредсказуемых изменений в трактовке законодательства регулятором.

Заключение: от бумажного комплаенса к архитектурному

Подводя итог, можно констатировать: цифровое законодательство 2026 года стирает грань между юридической службой и ИТ-департаментом. Как показывает анализ скрытых коллизий Цифрового кодекса, Закона об ИИ и обновленных норм о персональных данных, классический «бумажный» комплаенс не работает. Размытость формулировок и жесткость новых требований превращают алгоритмы, маркетинговые инструменты и внутренние базы данных в зоны повышенного правового риска. В этих условиях пассивное ожидание первых прецедентов и проверок становится опасной стратегией. Чтобы успешно развиваться в новой регуляторной реальности Казахстана компаниям необходимо перейти к концепции опережающего комплаенса — внедрять принципы прозрачности непосредственно в код алгоритмов (AI-by-Design), менять пользовательские интерфейсы и выстраивать архитектуру данных с учетом разных сценариев толкования закона.

Сауле Ахметова

Партнер,
GRATA International Казахстан, Алматы

sakhmetova@gratanet.com