

Бычкова Елена Сергеевна,
ассоциированный профессор Университета НАРХОЗ,
кандидат юридических наук

Кодекс Республики Казахстан
ЦИФРОВОЙ КОДЕКС РЕСПУБЛИКИ КАЗАХСТАН
(постатейный комментарий к некоторым статьям Кодекса)

I. Комментарий к статьям 3 - 13

РАЗДЕЛ 1. ОСНОВНЫЕ ПОЛОЖЕНИЯ
Глава 1. ОБЩИЕ ПОЛОЖЕНИЯ

Статья 3. Цель и задачи цифрового законодательства Республики Казахстан

1. Целью цифрового законодательства Республики Казахстан является обеспечение устойчивого развития и функционирования цифровой среды в интересах физических и юридических лиц, общества и государства.

2. Задачами цифрового законодательства Республики Казахстан являются:

1) правовое регулирование общественных отношений, возникающих в цифровой среде;

2) определение механизмов реализации единой государственной политики в цифровой среде;

3) укрепление законности и правопорядка в цифровой среде;

4) создание условий для привлечения инвестиций в развитие цифровой среды в Республике Казахстан;

5) правовое обеспечение цифровой трансформации всех сфер общественных отношений.

1. Как уже отмечалось в предисловии к настоящему Научно-практическому комментарию (уверена, что об этом будет сказано),

Цифровой Кодекс является основополагающим отраслевым актом, в соответствии с которым в Республике Казахстан должно формироваться законодательство, регулирующее отношения в цифровой среде, а также корректироваться уже действующее законодательство, не соответствующее подходам, установленным Кодексом.

На момент подготовки настоящего Комментария система цифрового законодательства Республики Казахстан включает Цифровой кодекс, Законы «О кибербезопасности», «Об искусственном интеллекте», «О цифровых активах», «Об онлайн-платформах и онлайн-рекламе», а также значительное количество подзаконных нормативных-правовых актов.

Цифровизация как системный процесс затрагивает все отрасли экономики и сферы общественной жизни, влияет на приоритеты государственной политики и направления международного сотрудничества. В этой связи отдельные положения гражданского, предпринимательского, финансового и иного законодательства также могут рассматриваться как элементы цифрового законодательства, если они регулируют отношения, возникающие в цифровой среде либо в связи с использованием цифровых технологий.

При этом цифровая среда рассматривается Цифровым кодексом не как изолированная технологическая сфера, а как **пространство возникновения общественных отношений по поводу создания, обращения, хранения, передачи и использования цифровых данных и цифровых объектов.**

Таким образом, Цифровой кодекс выполняет не только регулятивную, но и системообразующую функцию, формируя единые подходы к регулированию общественных отношений, возникающих в цифровой среде.

2. Определяя цель законодательного акта, разработчик формулирует стратегический ориентир, который отражает желаемое состояние регулируемых общественных отношений и основные направления государственной политики в соответствующей сфере, на достижение которых направлено правовое регулирование.

Закрепление устойчивого развития и функционирования цифровой среды в качестве ключевой цели развития казахстанского цифрового законодательства и правового регулирования отражает современные международные подходы регулирования, сопровождающие процессы цифровой трансформации.

Базовым ориентиром является Повестка дня в области устойчивого развития на период до 2030 года, принятая Генеральной Ассамблеей ООН, в которой закреплены согласованные подходы государств к достижению

целей устойчивого развития. В числе целей определены создание стойкой инфраструктуры, содействие всеохватной и устойчивой индустриализации и инновациям, которая заключается в обеспечении устойчивого экономического развития и повышения благосостояния через создание качественной, надежной и устойчивой инфраструктуры, развитие инклюзивной и устойчивой индустриализации, а также стимулирование инноваций, научных исследований и расширения доступа к технологиям¹.

Развитие идеи о том, что использование цифровых технологий должно способствовать достижению целей устойчивого развития, получило отражение и в документах ООН по цифровому сотрудничеству. Так, в докладе Генерального секретаря ООН «Дорожная карта по цифровому сотрудничеству» содержит и детализирует 5 пять наборов рекомендаций относительно того, каким образом международное сообщество может принять совместные меры в целях оптимизации использования цифровых технологий и снижения рисков:

- а) построение инклюзивной цифровой экономики и общества;
- б) укрепление человеческого и институционального потенциала;
- с) защита прав человека и его способности активно воздействовать на мир;
- д) содействие укреплению доверия, безопасности и стабильности в цифровом пространстве;
- е) содействие глобальному цифровому сотрудничеству².

Указанные направления нашли отражение не только в целях и задачах правового регулирования цифровой среды в Республике Казахстан, но и в принципах регулирования, закрепленных в статье 4 Цифрового кодекса.

С правовой точки зрения устойчивость цифровой среды предполагает наличие стабильного и предсказуемого правового регулирования в отношении цифровых данных и цифровых объектов, сбалансированное определение прав и обязанностей участников цифровой среды, а также наличие механизмов защиты их прав и законных интересов.

3. «Раскрывая содержание цели отраслевого законодательства, законодатель в ряде случаев также формулирует задачи соответствующей отрасли законодательства... Будучи моментом содержания цели, задачи

¹ Резолюция, принятая Генеральной Ассамблеей 25 сентября 2015 года. Преобразование нашего мира: Повестка дня в области устойчивого развития на период до 2030 года. Официальный сайт Организации объединенных наций. [Электронный ресурс]. URL: <https://docs.un.org/ru/A/RES/70/1> (дата обращения: 02.04.2026)

² Дорожная карта по цифровому сотрудничеству: осуществление рекомендаций Группы высокого уровня по цифровому сотрудничеству. Официальный сайт Организации объединенных наций. [Электронный ресурс]. URL: <https://docs.un.org/ru/A/74/821> (дата обращения: 02.04.2026)

отрасли законодательства конкретизируют цель, способствуя более точному ее пониманию субъектами правоприменительной деятельности и тем самым более эффективному ее достижению. Таким образом, достижение цели отраслевого законодательства осуществляется через реализацию его задач»³.

Если пункт 1 статьи 3 определяет стратегическую цель по созданию цифровой среды, ключевыми характеристиками которой являются устойчивое развитие и функционирование в интересах физических и юридических лиц, общества и государства, то пункт 2 определяет инструментальные подходы к достижению такой цели.

Подпункт 1) предусматривает в качестве задачи цифрового законодательства правовое регулирование общественных отношений, возникающих в цифровой среде. Важно отметить, что **законодатель определяет объектом правового регулирования не цифровые технологии сами по себе, а общественные отношения, возникающие в связи с их созданием, внедрением и использованием.** Цифровым кодексом и иными актами «цифрового законодательства» регулируются не только технические аспекты цифровизации, а более широкий круг общественных отношений, связанных с оборотом цифровых данных и цифровых объектов, реализацией прав личности в цифровой среде, использованием цифровых технологий государством и бизнесом, определением правового режима отдельных видов цифровых объектов и технологий.

С другой стороны, задача правового регулирования любых общественных отношений заключается в воздействии на них посредством юридических инструментов: установления правил поведения, определения прав и обязанностей субъектов отношений, юридической ответственности и порядка правоприменения.

Сфера цифровых технологий отличается высокой динамичностью развития, постоянной трансформацией и технологической сложностью, в следствие чего далеко не все аспекты использования технологий могут и должны становиться предметом правового регулирования. Так в сфере искусственного интеллекта значительная часть подходов к регулированию формируется через этические принципы и рекомендации международных организаций.

Закрепление рассматриваемой задачи выполняет не только регулятивную, но и также ограничительную функцию, направленную на предотвращение включения в цифровое законодательство оценочных,

³ Буянова М.О. Понятие и значение определения целей и задач отраслевого законодательства. Вестник ВГУ. Серия: Право. 2024. № 1 (56). [Электронный ресурс]. URL: <https://cyberleninka.ru/article/n/ponyatie-i-znachenie-opredeleniya-tseley-i-zadach-otraslevogo-zakonodatelstva> (дата обращения: 03.04.2026)

идеологических и декларативных положений. Задачи по определению механизмов реализации единой государственной политики в цифровой среде (пп. 2) и правовому обеспечению цифровой трансформации всех сфер общественных отношений (пп. 5) обусловлены тем, что процессы цифровизации охватывают не только экономику и общественную жизнь, но и систему государственного управления.

Развитие цифровой среды и экономики не может осуществляться фрагментарно, это требует согласованности на уровне стратегических задач государства, единых подходов к выработке регуляторной политики, правового регулирования, технических требований и стандартов.

Цифровой кодекс в данном процессе выполняет роль базового законодательного акта, закрепляющего ключевые принципы, подходы и понятийный аппарат, которые должны использоваться при дополнении отраслевого законодательства положениями, регулирующими отношения в цифровой среде.

Реализация указанных задач должна осуществляться как в плоскости правотворчества, так и правоприменения. В аспекте правотворчества это означает, что разработчики нормативных правовых актов, регулирующих отношения в цифровой среде, включая отраслевое законодательство, должны исходить из положений, принципов и подходов, закрепленных в Цифровом кодексе. Такой подход обеспечивает согласованность регулирования, предотвращает дублирование и конфликт норм, а также исключает формирование несогласованных правовых режимов в отдельных секторах цифровой экономики.

Органы государственной власти, суды и иные субъекты в процессе правоприменения положений, регулирующих отношения в цифровой среде, должны учитывать общие принципы и цели, закрепленные в Кодексе, обеспечивая единообразие практики и согласованность принимаемых решений.

4. Укрепление законности и правопорядка в цифровой среде является самостоятельной задачей «цифрового законодательства» Республики Казахстан.

Отношения в цифровой среде – формирующаяся реальность, многие проявления которой еще не получили достаточного регулирования правом. Можно обоснованно констатировать, что право во многом не успевает за развитием технологий. Цифровая среда порождает новые формы взаимодействия, поведения и рисков, которые не всегда можно урегулировать традиционными правовыми механизмами.

В сфере гражданско-правовых отношений в действующем гражданском законодательстве Республики Казахстан отсутствуют

положения, которые бы в достаточной степени определяли моменты возникновения, изменения и прекращения прав и обязанностей субъектов цифровых отношений, применимое право в отношении трансграничных сделок, действительность сделок, совершаемых с использованием цифровых технологий и пр. Особую сложность представляет определение правового режима результатов, создаваемых автономными технологиями, способными действовать и принимать решения без непосредственного участия человека.

Особую актуальность в этой связи приобретает дальнейшее развитие правовой доктрины и модернизация отдельных институтов гражданского законодательства Республики Казахстан применительно к цифровой среде. Развитие цифрового оборота объективно требует адаптации традиционных правовых конструкций к новым объектам правоотношений, включая цифровые данные, цифровые объекты, цифровые активы и иные результаты цифровой деятельности.

В публично-правовой сфере задача по укреплению законности заключается, в частности, в обеспечении баланса между внедрением технологий и соблюдением прав и свобод граждан и юридических лиц. Расширение цифровых государственных сервисов, использование больших данных и алгоритмических решений в государственном управлении требуют недопущения произвольного вмешательства в частную жизнь и создания недискриминационных практик.

Указанная задача связана с принципами соблюдения прав и свобод человека в цифровой среде, безопасности цифровой среды и баланса частных и публичных интересов, закрепленными в статьях 5, 6 и 9 Цифрового кодекса.

Развитие цифровых технологий сопровождается не менее интенсивным ростом киберпреступности. Укрепление правопорядка в цифровой среде предполагает соответствующую квалификацию правонарушений с использованием технологий, разработку мер ответственности, а также совершенствования механизмов выявления, пресечения и расследования правонарушений.

Особое значение имеют превентивные меры обеспечения правопорядка в цифровой среде: установление требований к поведению субъектов цифровой среды, техническим параметрам функционирования цифровых объектов, включая требования к кибербезопасности, защите данных, надежности инфраструктуры и устойчивости сервисов.

Кроме того, укрепление законности и правопорядка в цифровой среде связано с обеспечением защиты публичных интересов, устойчивости цифровой инфраструктуры и цифрового суверенитета государства. Нарушения в цифровой среде способны затрагивать не только права

отдельных лиц, но и интересы общества и государства в целом, что требует комплексного подхода к правовому регулированию цифровых отношений.

Таким образом, укрепление законности и правопорядка в цифровой среде предполагает формирование комплексной системы правового регулирования, сочетающей адаптацию или корректировку действующих правовых режимов, разработку новых правовых правил с учетом технологических особенностей цифровых объектов и технологий, а также обеспечением баланса между технологическим развитием, защитой прав личности и охраной публичных интересов.

5. Создание в Казахстане благоприятной институциональной, правовой и деловой среды является одним из ключевых направлений государственной политики, неоднократно обозначавшейся Главой государства в программных документах и официальных выступлениях.

«Казахстан одним из первых в мире внедрил гибкое и современное цифровое регулирование. Принят Цифровой кодекс, вступил в силу Закон «Об искусственном интеллекте». Однако это лишь начало масштабного пути, и мы не должны на этом останавливаться. Мир вошел в эпоху динамичных технологических изменений. Об этом вам хорошо известно. Наука, образование и технологии развиваются высокими темпами, а значит и нормативная база требует оперативного обновления»⁴.

Основные направления и задачи по развитию инвестиционной политики определены в Концепции инвестиционной политики Республики Казахстан до 2030 года.

Дополнительное значение имеет закрепленный в Общенациональной стратегии Digital Qazaqstan принцип экономической эффективности, согласно которому цифровая трансформация должна способствовать созданию новых рынков, повышению производительности и развитию экономики. В связи с этим наличие стабильного и предсказуемого правового регулирования является важным условием привлечения инвестиций и реализации цифровых проектов.

В этом контексте задачей цифрового законодательства является формирование такого правового режима, который обеспечивал бы понятные и стабильные условия для ведения деятельности в цифровой среде, а также гарантии защиты прав инвесторов и участников рынка.

Так, отдельные положения Цифрового кодекса уже направлены на реализацию данной задачи. Прежде всего, это закрепленные в статье 4 принципы правового регулирования: свобода обращения цифровых

⁴ Глава государства провел совещание по проекту Digital Qazaqstan. Официальный сайт Президента Республики Казахстан. [Электронный ресурс]. URL: <https://www.akorda.kz/ru/glava-gosudarstva-provel-soveshchanie-po-proektu-digital-qazaqstan-1325054> (дата обращения: 03.04.2026)

данных, свобода создания, развития и применения технологий, баланс частных и публичных интересов, технологическая нейтральность правового регулирования.

Кроме того, закрепление правовых режимов цифровых объектов и цифровых данных в качестве объектов гражданского оборота, а также определение прав и обязанностей их собственников и владельцев обеспечивает правовую определенность, что позволяет участникам рынка понимать возможности по распоряжению такими объектами.

Следует отметить, что Казахстан в числе первых стран, закрепивших на уровне кодифицированных актов комплексный подход правового регулирования цифровой среды. Это дает дополнительные гарантии системности, предсказуемости и прозрачности регулирования.

Таким образом, задача по созданию в Казахстане условий для привлечения инвестиций в развитие цифровой среды имеет координационное значение и должна учитываться как при разработке нормативных правовых актов, так и в процессе правоприменения.

Статья 3 Цифрового кодекса имеет ключевое значение для понимания целей формирования и места «цифрового» законодательства в правовой системе Республики Казахстан. Закрепленные в ней цель и задачи определяют основные направления развития законодательства, содержание государственной политики в сфере цифровизации и подходы к толкованию норм Кодекса.

Статья 4. Принципы цифрового законодательства Республики Казахстан

Правовое регулирование общественных отношений в цифровой среде основывается на следующих основных принципах:

- 1) соблюдение прав, свобод и законных интересов человека в цифровой среде;*
- 2) безопасность человека, общества и государства при применении цифровых технологий;*
- 3) свобода обращения цифровых данных;*
- 4) свобода создания, развития и применения цифровых технологий;*
- 5) баланс частных и публичных интересов;*
- 6) доступность и инклюзивность цифровой среды;*
- 7) пропорциональное и обоснованное участие государства в цифровой среде;*
- 8) технологическая нейтральность правового регулирования;*
- 9) цифровая этика и социальная ответственность.*

1. Статьей 4 Цифрового кодекса определены основные принципы, в соответствии с которыми должно формироваться регулирование общественных отношений в цифровой среде.

Принципы правового регулирования – это фундаментальные, руководящие начала, определяющие суть, направленность и пределы воздействия права на общественные отношения.

Обязательное включение принципов регулирования и описание механизмов их реализации предусмотрено статьей 14-3 Закона «О правовых актах».

Основная цели и значение норм-принципов, содержащихся в статьях 4-13 Цифрового кодекса, заключается в обеспечении системности регулирования отношений в цифровой среде и формировании единых подходов для всего казахстанского законодательства, регулирующего отношения в цифровой среде.

Законом «О правовых актах» (п. 3 ст. 14-3) установлено требование о соответствии норм законов установленных в них принципам. Соответственно, положения нормативных правовых актов, регулирующих отношения в цифровой среде, должны толковаться и применяться с учетом принципов, определенных Цифровым кодексом как ключевым отраслевым законодательным актом.

В связи с принятием Цифрового кодекса, нормы ранее принятых законодательных актов, не соответствующие закрепленным в нем принципам и подходам регулирования, могут требовать корректировки.

2. Значение закрепленных в Цифровом кодексе принципов необходимо оценивать с учетом правовой природы отношений, возникающих в цифровой среде. Существенная часть таких отношений является гражданско-правовой по своей природе, поскольку складывается по поводу создания, использования, передачи, хранения и защиты цифровых данных, а также осуществления прав на цифровые объекты.

Цифровая среда является областью гражданско-правовых отношений, в рамках которой правоотношения складываются по поводу цифровых данных, а права на разнообразные цифровые объекты возникают и передаются с использованием цифровых технологий.

Сами цифровые объекты являются объектами гражданских прав, права на которые могут переходить на основании гражданско-правового договора (пункт 2 статьи 1 и пункт 4 статьи 38 Цифрового кодекса), если: (i) оборот каких-то цифровых объектов или их видов не запрещен или не ограничен законом (в частности, в самом Цифровом кодексе, например, в соответствии пунктом 3 статьи 21 идентификационные цифровые данные не являются оборотоспособным имуществом, а оборот распределенных цифровых объектов и национальных цифровых объектов запрещен пунктом 5 статьи 26 и пунктом 3 статьи 34, соответственно), либо (ii) они представляют собой неимущественное / нематериальное благо (как, к примеру, идентификационная цифровая запись согласно пункту 3 статьи 21 и цифровая идентичность согласно пункту 1 статьи 40), права на которые подлежат правовой защите в качестве личных [неимущественных] прав (как, например, права субъекта цифровых данных в соответствии с пунктом 4 статьи 37 и цифровая идентичность в соответствии с тем же пунктом 3 статьи 40).

В свою очередь, согласно пункту 1 статьи 1 ГК, такие имущественные и личные неимущественные отношения, включая защиту имущественных и личных [неимущественных] прав, регулируются гражданским законодательством. В связи с этим та часть (и она является преобладающей) цифровой среды, в которой реализуются гражданские правоотношения, основанные на равенстве участников, своей правовой основой имеет гражданское законодательство. Соответственно, правовое регулирование этих отношений в цифровой среде осуществляется на началах гражданского законодательства, закрепленных в статье 2 ГК, с применением презумпций и правил осуществления гражданских прав, установленных в статье 8 ГК, и подлежащих защите как предусмотрено в статьях 9 и 10 ГК.

С учетом этого, перечисляемые в комментируемой статье принципы следует рассматривать, помимо разъясняемого в данном комментарии, как подлежащие соблюдению, во-первых, в той части, которая не приводит к нарушению или иному умалению основных начал гражданского законодательства и(или) игнорированию установленных в ГК презумпций поведения субъектов гражданского оборота (включая субъектов цифровой среды), и во-вторых, как принципы использования применяемых в цифровой среде цифровых технологий для обеспечения формирования, использования, передачи цифровых данных, обеспечения правомерного доступа к ним и защите прав субъектов цифровых данных.

В тексте Комментария неоднократно упоминается такая особенность отношений в цифровой среде как высокая динамика их развития и трансформации, а также ограниченная возможность предварительного определения рисков и последствий технологических изменений. Соответственно, законодательство объективно не может детально урегулировать все возникающие общественные отношения. В таких условиях именно принципы становятся наиболее устойчивым механизмом регулирования.

Любые законодательные нововведения должны в первую очередь оцениваться на предмет их соответствия принципам регулирования. В этой связи принципы регулирования отношений в цифровой среде обеспечивают устойчивость, системность и предсказуемость регулирования. Они позволяют распространять единые регуляторные подходы на новые технологические явления без необходимости постоянного внесения изменений в законодательство.

Принципы регулирования имеют особое значение и для судебного толкования. В случаях, когда спорные правоотношения прямо не урегулированы законодательством на основании принципов может оцениваться допустимости действий участников отношений в цифровой среде и пределов государственного вмешательства.

Например, при возникновении спора о допустимости использования новой технологии, прямо не урегулированной законодательством, правоприменитель может руководствоваться принципом технологической нейтральности, оценивая не саму технологию, а последствия ее использования для прав и законных интересов субъектов цифровой среды.

Следует отметить, что принципы, включенные в статью 4 кодекса, отражают не субъективное усмотрение казахстанского законодателя, а в значительной степени основаны на сформировавшихся международных подходах к регулированию цифровой среды.

В комментарии к отдельным статьям приведена информация о международных актах и документах, которые послужили концептуальной

основой соответствующих принципов. том, в соответствии с какими международными актами разработан принцип. Такая материалы могут быть использованы как дополнительный источник доктринального толкования в случаях, когда национальная правоприменительная практика еще не сформирована.

Так, закрепленный в статье 5 Кодекса принцип, согласно которому высшей ценностью являются права, свободы и законные интересы человека в цифровой среде соответствует положениям Всеобщей декларации прав человека, Международного пакта о гражданских и политических правах, резолюциям Совета ООН по правам человека «Поощрение, защита и осуществление прав человека в Интернете».

Принципы безопасности, пропорциональности государственного участия, технологической нейтральности и недискриминации отражены в таких европейских актах, регулирующих цифровую среду, которые являются ориентиром для разработчиков цифрового регулирования в разных юрисдикциях: Digital Services Act, Digital Markets Act, Европейский кодекс электронных коммуникаций, Рекомендации ЮНЕСКО по этике искусственного интеллекта и других документах.

Принципы, указанные в статье 4, можно сгруппировать по функциональное направленности и целям правового регулирования:

1) Правозащитная направленность: соблюдение прав, свобод и законных интересов человека в цифровой среде; безопасность человека, общества и государства при применении цифровых технологий. Цель – защита человека как высшей ценности в цифровой среде.

2) Направленность на развитие цифровой экономики: свобода обращения цифровых данных; свобода создания, развития и применения цифровых технологий. Общая цель – создать условия для развития цифровой экономики и инноваций, а также конкуренции на цифровых рынках.

3) Направленность на создание сбалансированного взаимодействия между субъектами цифровых отношений: баланс частных и публичных интересов; пропорциональное и обоснованное участие государства в цифровой среде.

Социальная направленность в целях создания равного доступа к цифровым благам: доступность и инклюзивность цифровой среды. Целью является обеспечение равного доступа граждан к цифровым благам, цифровым услугам и возможностям цифровой экономики независимо от возраста, места проживания, состояния здоровья, уровня доходов и иных обстоятельств.

4) Регуляторная направленность: технологическая нейтральность правового регулирования. Цель – обеспечение гибкости, устойчивости и предсказуемости правового регулирования.

5) Этическая направленность: цифровая этика и социальная ответственность. В целях обеспечения морально-этических стандартов и доверия к цифровым технологиям.

Закрепленные в статье 4 принципы формируют основу правового регулирования цифровой среды. Соблюдение закрепленных в Цифровом кодексе принципов при разработке проектов нормативных правовых актов, стратегических и рекомендательных документов, а также в правоприменительной и судебной практике обеспечит всестороннюю защиту прав человека, системность регулирования, его предсказуемость, что в свою очередь отразится на устойчивости и цифровой среды и создаст благоприятные условия для развития технологий и цифровой экономики.

При этом, принципы цифрового законодательства не существуют изолированно от общей системы законодательства Республики Казахстан. Их применение должно осуществляться во взаимосвязи с конституционными принципами, основными началами гражданского законодательства, принципами регулирования предпринимательской деятельности.

Статья 5. Соблюдение прав, свобод и законных интересов человека в цифровой среде

1. Права, свободы и законные интересы человека в цифровой среде признаются высшей ценностью, и их ограничение возможно только законами Республики Казахстан и лишь в той мере, в какой это необходимо в целях защиты конституционного строя, охраны общественного порядка, прав и свобод человека, здоровья и нравственности населения.

2. Отношения в цифровой среде основываются на свободном, осознанном и выраженном волеизъявлении человека.

3. Алгоритмические и автоматизированные решения, затрагивающие права, свободы и законные интересы человека в цифровой среде, применяются с соблюдением прозрачности, недискриминации и возможности контроля со стороны субъекта цифровой среды.

1. Цифровой кодекс Республики Казахстан регулирует новые по своей сути общественные отношения и является новаторским актом с точки зрения подходов к правовому регулированию технологий. Ряд его положений, прежде всего, принципы и подходы к регулированию, ранее не закреплялись в казахстанском законодательстве и не имеют устоявшегося понимания и толкования. В этой связи отдельные положения Кодекса должны толковаться с учетом международных актов, к которым присоединилась Республика Казахстан и приняла на себя соответствующие обязательства, а также ряда международных документов рекомендательного характера как дополнительного источника толкования. В большей степени это относится к сфере защиты прав человека, а также соблюдения инклюзии в цифровой среде, где международные акты содержат более детальные формулировки и подходы, что позволяет более последовательно и определенно раскрывать содержание норм национального законодательства.

Пунктом 2 статьи 2 Цифрового кодекса прямо предусмотрено, что международные договоры, ратифицированные Республикой Казахстан, имеют приоритет перед настоящим Кодексом. Принцип приоритета прав и свобод человека в цифровой среде закреплён рядом международных документов, к которым присоединилась Республика Казахстан.

2. Закреплённый в статье 5 принцип приоритета прав и свобод человека в цифровой среде является проявлением принципа верховенства права (Rule of Law), согласно которому права человека выступают основным ориентиром при разработке, применении и толковании законодательства, в том числе, регулирующего отношения в цифровой среде.

Данный пункт отражает подходы, сформированные в международном праве. Основой выступает Всеобщая декларация прав человека ООН 1948 года⁵, положения которой применимы и к цифровой среде. ВДЧП устанавливает право каждого человека на неприкосновенность частной жизни, свободу убеждений и их выражения, защиту от дискриминации, а также право на участие в культурной жизни.

Аналогичные подходы закреплены в Международном пакте о гражданских и политических правах⁶ (ратифицирован РК в 1994 году), гарантирующем свободу выражения с возможными ограничениями в целях: *«а) уважения прав и репутации других лиц; б) для охраны государственной безопасности, общественного порядка, здоровья или нравственности населения»* (ст. 19).

Международный пакт о экономических, социальных и культурных правах 1976⁷ года (ратифицирован РК в 1994 году) закрепляет право каждого на защиту моральных и материальных интересов, возникающих в связи с созданием научных, литературных или художественных произведений, что приобретает особое значение в цифровой среде.

Резолюции Совета ООН по правам человека «Поощрение, защита и осуществление прав человека в Интернете» (перечислены далее) прямо ссылаются на ВДЧП и Пакты, подтверждая их применение в цифровой среде.

Практическое значение рекомендательных документов ООН очень верно по мнению автора сформулировано в статье 5 Руководящих принципов: *«Руководящие принципы могут служить ресурсом для целого ряда заинтересованных сторон: директивных органов при определении законных целей и принципов в области прав человека, а также инклюзивных и партисипативных процессов, которые могут учитываться при разработке политики; контрольно-надзорных и других органов регулирования, занимающихся реализацией и оценкой политики, кодексов поведения или регулирования; цифровых платформ в их политике и практике; и других заинтересованных сторон, таких как гражданское*

⁵ Всеобщая декларация прав человека. Принята резолюцией 217 А (III) Генеральной Ассамблеи ООН от 10 декабря 1948 года. [Электронный ресурс]. URL: <https://adilet.zan.kz/rus/docs/O4800000001> (дата обращения: 22.04.2026)

⁶ Международный пакт о гражданских и политических правах. Принят резолюцией 2200 А (XXI) Генеральной Ассамблеи от 16 декабря 1966 года. Официальный сайт Организации объединенных наций. [Электронный ресурс]. URL: https://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml (дата обращения: 22.04.2026)

⁷ Международный пакт об экономических, социальных и культурных правах. Принят резолюцией 2200 (XXI) Генеральной Ассамблеи от 16 декабря 1966 года. Официальный сайт Организации объединенных наций. [Электронный ресурс]. URL: https://www.un.org/ru/documents/decl_conv/conventions/pactecon.shtml (дата обращения: 22.04.2026)

общество, в их усилиях по ведению информационно-разъяснительной работы и обеспечению подотчетности. СМИ также могут воспользоваться этими рекомендациями в своей работе по привлечению к ответственности влиятельных лиц».

На национальном уровне человекоцентричный подход отражен в Общенациональной стратегии Digital Qazaqstan, согласно которой цифровая трансформация должна быть ориентирована на повышение качества жизни граждан, обеспечение их благополучия и расширение возможностей на протяжении всей жизненной траектории человека.

3. В пункте 1 комментируемой статьи определены основания, при которых допускается законодательное ограничение прав, свобод и законных интересов человека в цифровой среде.

В широком смысле эти ограничения обусловлены принятыми в нашей стране нравственностью и социальным порядком. Для применения этих ограничений в правовой сфере (включая правовое регулирование цифровой среды) существует юридический термин – публичный порядок (*ordre public* / *public order* / *public policy*). Его значение заключается не столько в том, чтобы отказать в применении правовых норм или не допустить применения правовых норм (включая нормы международных договоров), сколько не позволить негативных последствий их применения для основ государственности данной страны и признаваемого в ней публичного интереса. Поскольку же этот термин (публичный порядок). объективно является общим, абстрактным и относительным понятием, то в каждом конкретном случае угроза публичному порядку определяется судьями, в том числе судьями конституционного суда (когда угроза публичному порядку (тем же конституционным основам) содержится в принимаемых государственными органами правовых актах).⁸

Это понятие используется и в казахстанском праве (в том числе в нормах ГК и законодательстве об арбитраже) как юридический термин.

Несмотря на то, что пункт 1 комментируемой статьи преимущественно адресован законодателю и регуляторам, соответствие принимаемых ими актов содержанию этого пункта будет определяться судебским усмотрением и резолюциями Конституционного Суда Республики Казахстан, являющимися органами, которые в своей деятельности и при осуществлении своих полномочий руководствуются именно правовыми понятиями.

Кроме того, такие критерии, как используемые в комментируемой статье «охрана общественного порядка, права и свобода человека, здоровье

⁸ Thoma I. Public policy (*ordre public*). Encyclopedia of Private International Law. Jü. Basedow, G. Rühl, F. Ferrari and P. de Miguel Asensio, Eds. Edward Elgar Publishing, 2017. Vol. 2, 1854 p. P. 1453–1459

и нравственность населения» являются слишком широкими, позволяя ограничение свободы даже в тех случаях, когда угрозу публичному интересу и(или) публичному порядку идентифицировать невозможно или не обоснованно, а проявление частного произвола является очевидным.

В связи с этим, представляется целесообразным при применении пункта 1 комментируемой статьи исходить из того, что предусмотренные к нем цели «защиты конституционного строя, охраны общественного порядка, прав и свобод человека, здоровья и нравственности населения» означают публичный порядок Республики Казахстан и не допускают трактование этих целей иным образом, чем общепризнанное в мировой практике понятие публичного порядка.⁹

4. Статья 5 Цифрового кодекса определяет фундаментальный подход, который закреплен во многих международных документах и используется как основа для разработки регулирования цифровой среды, включая казахстанское законодательство: **права и свободы человека, принадлежащие ему в офлайн-среде, должны в равной степени защищаться и в цифровой среде.** Такой подход определен в ряде резолюций Совета ООН по правам человека «Поощрение, защита и осуществление прав человека в Интернете». Впервые он был сформулирован в резолюции от 29 июля 2012 года A/HRC/20/L.13¹⁰, в которой Совет подтвердил, что те же права, которыми человек обладает в офлайн-среде, должны защищаться и в онлайн-среде. В последующих резолюциях A/HRC/RES/26/13¹¹, A/HRC/32/13¹² и A/HRC/RES/47/16¹³ данный подход был подтвержден: *«те же самые права, которые человек имеет в офлайновой среде, должны также защищаться в онлайновой среде, в частности свобода выражения мнений, которая применима независимо от границ и в рамках любых выбираемых человеком средств*

⁹ См. Карагусов Ф. О легальной дефиниции «Основы правопорядка Республики Казахстан». Интернет-ресурс https://online.zakon.kz/Document/?doc_id=39342132&pos=6;-110#pos=6;-110; Karagussov F. About a Concept of Ordre Public in Law of Kazakhstan. Интернет-ресурс https://online.zakon.kz/Document/?doc_id=34304654&pos=6;-110#pos=6;-110 Дата обращения 15.04.2025

¹⁰ Резолюция, принятая Советом ООН по правам человека 29 июня 2012 года «Поощрение, защита и осуществление прав человека в Интернете». Официальный сайт Организации объединенных наций. [Электронный ресурс]. URL: <https://docs.un.org/ru/A/HRC/20/L.13> (дата обращения: 15.04.2026)

¹¹ Резолюция, принятая Советом ООН по правам человека 14 июля 2014 года «Поощрение, защита и осуществление прав человека в Интернете». Официальный сайт Организации объединенных наций. [Электронный ресурс]. URL: <https://docs.un.org/ru/A/HRC/RES/26/13> (дата обращения: 21.04.2026)

¹² Резолюция, принятая Советом ООН по правам человека 18 июля 2016 года «Поощрение, защита и осуществление прав человека в Интернете». Официальный сайт Организации объединенных наций. [Электронный ресурс]. URL: <https://docs.un.org/ru/A/HRC/RES/32/13> (дата обращения: 21.04.2026)

¹³ Резолюция, принятая Советом ООН по правам человека 26 июля 2021 года «Поощрение, защита и осуществление прав человека в Интернете». Официальный сайт Организации объединенных наций. [Электронный ресурс]. URL: <https://docs.un.org/ru/a/hrc/res/47/16> (дата обращения: 21.04.2026)

массовой информации, в соответствии со статьями 19 Всеобщей декларации прав человека и Международного пакта о гражданских и политических правах».

Указанный подход стал основой для международного регулирования прав человека в цифровой среде. Хотя в Цифровом кодексе он прямо не сформулирован, его можно вывести из системного толкования положений Кодекса и иных актов, регулирующих отношения в цифровой среде. В этой связи статья 5 Кодекса должна рассматриваться **не как перечень прав и свобод, подлежащих защите в цифровой среде, а как общая гарантия того, что любые положения Цифрового кодекса должны толковаться через призму защиты прав и свобод человека, а проекты актов «цифрового законодательства» Республики Казахстан должны разрабатываться с учетом этого принципа.**

5. Пункт 2 статьи 5 закрепляет принцип свободы волеизъявления человека в цифровой среде как один из ключевых механизмов защиты личности от возможных ограничений и злоупотреблений со стороны собственников цифровых объектов, разработчиков технологий, а также от чрезмерного воздействия алгоритмов и систем ИИ.

Аналогичный подход определен Законом РК «Об искусственном интеллекте», где свобода воли человека напрямую указана как важный фактор функционирования и регулирования отношений с использованием ИИ: *«Человек, его жизнь, права и свободы рассматриваются как высшая ценность в процессах создания и эксплуатации систем искусственного интеллекта. При эксплуатации систем искусственного интеллекта должно быть обеспечено сохранение автономии и свободы воли человека в принятии им решений»* (ст. 9).

Закрепление свободы волеизъявления обусловлено также признанием цифровой среды областью гражданских правоотношений, и в своём содержании соответствует общим началам гражданского законодательства, закрепленным в статье 2 ГК.

В то же время, с учетом пункта 1 статьи 36 Цифрового кодекса (согласно которому субъектами цифровой среды могут быть физические и юридические лица, а также иные лица, обладающие цифровой идентичностью) в комментируемой статье закрепляется частная автономия любого субъекта, являющегося в соответствии с Цифровым кодексом субъектом цифровой среды.

Вместе с тем, свобода волеизъявления в цифровой среде с точки зрения научной доктрины не является достаточно проработанным вопросом в аспекте правовой природы и содержания волеизъявления (свобода выбора, распоряжения и пр.), пределов реализации такой свободы в разных правоотношениях, места такой свободы в системе прав и свобод человека,

ответственности за нарушение и пр. В этой связи на момент подготовки настоящего комментария особое значение для толкования имеют положения отдельных международных актов, а также принцип, согласно которому **права и свободы человека, принадлежащие ему в офлайн-среде, должны в равной степени защищаться и в цифровой среде.**

Право на свободное волеизъявление детализировано в некоторых статьях Кодекса и иных актах казахстанского законодательства, регулирующих отношения в цифровой среде:

- субъект персональных данных вправе требовать удаления, анонимизации или ограничения обработки своих персональных данных, размещенных или обрабатываемых в цифровой среде, независимо от основания их получения, за исключением случаев, предусмотренных законами Республики Казахстан (п. 1 ст. 41 ЦК);

- никто не может быть принужден к цифровой идентификации, за исключением случаев, когда такая обязанность прямо предусмотрена законами Республики Казахстан (п. 2. ст. 40 ЦК);

- субъект цифровых данных обладает правомочиями в отношении этих цифровых данных, включая право на доступ к ним, контроль, удаление, ограничение обработки, а также на получение информации о целях, правовых основаниях и способах обработки цифровых данных (п. 4 ст. 47 ЦК).

Пунктом 3 статьи 17 Закона «Об искусственном интеллекте» гарантирована защита свободы волеизъявления путем установки запрета на создание и эксплуатацию в Казахстане систем ИИ, обладающих функциональными возможностями по использованию подсознательных, манипулятивных или иных методов, искажающих поведение физического лица и ограничивающих способность принимать осознанные решения или вынуждающих принимать решения, которые могут причинить вред или создать угрозу причинения вреда.

Приведенное положение Закона отражает подпункт а) пункта 1 статьи 5 Регламента Европейского союза об искусственном интеллекте (AI Act)¹⁴: *«1. Следующие методы искусственного интеллекта запрещены: размещение на рынке, ввод в эксплуатацию или использование системы ИИ, которая разворачивает подсознательные методы за пределами сознания человека, или целенаправленно манипулятивные или обманчивые методы, с целью или эффекта существенного искажения поведения человека или группы лиц путем значительного ухудшения их способности принимать*

¹⁴ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending certain Union legislative acts (Artificial Intelligence Act). An official web-site of the European Union. [Электронный ресурс]. URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> (дата обращения: 27.04.2026).

обоснованное решение, тем самым заставляя их принять решение, которое они в противном случае не приняли бы таким образом, который причиняет или имеет разумную вероятность причинить этому лицу, другому лицу или группе лиц значительный вред». Положения Регламента могут быть применимы к казахстанским субъектам, в случае если их системы ИИ работают на рынке Европейского союза или затрагивает пользователей в ЕС.

В сфере персональных данных свобода волеизъявления реализуется прежде всего через институт согласия субъекта. В Законе РК «О персональных данных и их защите» согласие (волеизъявление) определяется как разрешение субъекта на сбор и обработку данных и используется как основное юридическое основание для обработки персональных данных. Одновременно, статьей 19 Закона РК «О персональных данных и их защите» предусмотрен запрет на автоматизированную обработку персональных данных, в результате которой у субъекта возникают, изменяются или прекращаются права, законные интересы – то есть, если субъект не выразил свое согласие (волеизъявление).

В то же время, согласие пользователя на обработку персональных данных не может считаться осознанным, если информация о целях обработки скрыта в пользовательском соглашении и не доведена до пользователя в понятной форме.

Для сравнения, GDPR определяет согласие следующим образом: (11) *«Согласие субъекта данных – это добровольное, конкретное, информированное и однозначное волеизъявление, в котором субъект данных с помощью заявления или четкого утвердительного действия дает согласие на обработку своих персональных данных»¹⁵.*

Требования GDPR должны соблюдать все казахстанские субъекты, которые обрабатывают персональные данные пользователей Европейского Союза.

В официальных разъяснениях GDPR Европейского совета по защите персональных данных дано уточнение относительно добровольности (свободы волеизъявления) при даче согласия: *«В целом, согласие может быть законным основанием только в том случае, если субъекту данных предоставляется контроль и реальный выбор в отношении принятия или*

¹⁵ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation – GDPR). An official web-site of the European Union. [Электронный ресурс]. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679> (дата обращения: 28.04.2026)

отклонения предложенных условий или отказа от них без ущерба для него»¹⁶.

На основании изложенного, можно сделать вывод, что **право свободного волеизъявления в цифровой среде предполагает наличие у субъекта выбора поведения, а также возможности давать согласие, требовать прекращения каких-либо действий или процессов в цифровой среде, а также защищать свои права.**

6. Указание в пункте 2 статьи 5 на осознанность волеизъявления человека означает, что лицо должно не просто формально совершить определенное действие или выразить согласие, но понимать содержание, юридические последствия и риски своих действий. Применительно к цифровой среде это предполагает обязательное ознакомление с условиями пользовательских соглашений, правилами сбора информации о действиях лица при пользовании цифровым ресурсом, условиями сбора и обработки персональных данных и пр.

Как уже отмечалось, аналогичный подход закреплён в GDPR, где согласие субъекта данных определяется как добровольное, конкретное, информированное и однозначное волеизъявление.

По сути, требование осознанности предполагает двустороннюю правовую обязанность: человек обязан ознакомиться с условиями цифрового взаимодействия, а собственники цифровых объектов, провайдеры услуг, субъекты, осуществляющие сбор персональных данных обязаны обеспечить возможность ознакомления с такой информацией в понятной и доступной форме. Так, пунктом 5 статьи 29 Кодекса прямо установлена обязанность владельцев цифровых платформ обеспечивать прозрачность условий использования, выраженных в пользовательском соглашении. В отношении иных цифровых объектов и сервисов данное требование вытекает из общего содержания пункта 2 статьи 5.

Предоставление возможности ознакомиться с информацией означает, в том числе, и требование о предоставлении информации на соответствующем языке, а также в случаях, предусмотренных законодательством – соблюдение требований в отношении лиц с инвалидностью.

7. Выражение волеизъявления в цифровой среде осуществляется дистанционно без использования устной речи или письменных подтверждений путем нажатия или выбора опции, то есть путем совершения действий в интерфейсе цифрового объекта. Именно поэтому

¹⁶ Guidelines 05/2020 on consent under Regulation 2016/679. An official web-site of the European Data Protection Board. [Электронный ресурс]. URL: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en (дата обращения: 28.04.2026).

для признания такого волеизъявления юридически значимым требуется установление дополнительных гарантий, позволяющих удостовериться, что цифровое подтверждение соответствует реальной воле человека.

По этой причине цифровая среда требует специальных механизмов подтверждения личности и волеизъявления.

Цифровым кодексом предусмотрено несколько обязательных условий для возникновения, изменения или прекращения правоотношений, к которым относятся цифровая аутентификация и цифровое подтверждение. Статья 47 Кодекса определяет понятие цифрового подтверждения и открытый перечень способов цифрового подтверждения.

Дополнительные требования содержатся в международных актах. Так, Recital 32 GDPR содержит дополнительное уточнение, согласно которому молчание, заранее отмеченные чекбоксы или бездействие не должны рассматриваться как согласие.

8. Алгоритмические и автоматизированные решения требуют особого правового регулирования и контроля, поскольку способны ограничивать права субъектов, создавать дискриминационные условия, нарушать принципы справедливости и равенства. В цифровой среде именно такие решения все чаще используются при предоставлении услуг, оценке поведения, обработке данных, принятии коммерческих решений, что объективно требует дополнительных гарантий защиты прав человека.

Пункт 3 статьи 5 Цифрового кодекса, устанавливающий требования к алгоритмическим и автоматизированным решениям, затрагивающим права, свободы и законные интересы человека в цифровой среде, отражает закрепление подходов международного права в национальном законодательстве.

Так, пункт 38 Рекомендаций ЮНЕСКО об этических аспектах искусственного интеллекта устанавливает, что *«людям следует дует предоставлять полную информацию о том, какие решения принимаются с использованием алгоритмов искусственного интеллекта или на основе полученных с их помощью данных, в том числе решения, затрагивающие их безопасность и права человека, чтобы в соответствующих случаях люди имели возможность запросить у субъектов ИИ или государственных учреждений пояснительную информацию. Кроме того, люди должны иметь возможность доступа к обоснованию затрагивающего их права и свободы решения и представлять заявления уполномоченным сотрудникам частных компаний или государственных учреждений, которые могут пересмотреть и изменить это решение. Субъектам ИИ следует надлежащим образом и своевременно информировать пользователей о*

том, предоставляется ли тот или иной продукт или услуга напрямую или с помощью ИИ-систем»¹⁷.

Регламент Европейского союза об искусственном интеллекте (AI Act) запрещает использование отдельных видов ИИ-систем, включая системы для социального оценивания физических лиц, если это ведет к неблагоприятным последствиям для их прав и свобод (ст. 5). В 2026 году вступает в силу дополнительная статья 86 Регламента, которая устанавливает право лица, в отношении которого принято решение, высокорисковой системой ИИ, получить ясные и содержательные пояснения роли системы ИИ в принятии решения¹⁸.

Схожие подходы закреплены в статье 22 GDPR «Автоматизированное принятие решений в индивидуальных случаях, в том числе профилирование» предусматривает право лица не подчиняться решению, основанному исключительно на автоматизированной обработке, если такое решение имеет юридические последствия или существенно затрагивает человека за исключением отдельных случаев¹⁹.

Принцип, закрепленный в пункте 3 статьи 5, включая требования о прозрачности, недискриминации и возможности контроля со стороны субъекта, развивается и в национальном законодательстве. Цифровой кодекс (ст. 43) предусматривает право субъекта, в отношении которого принимается полностью автоматизированное алгоритмическое решение, получить информацию о факте применения алгоритмической системы; получить объяснение ключевых факторов и критериев, повлиявших на решение, без раскрытия алгоритмов, исходного кода или сведений, составляющих охраняемую законом тайну; потребовать пересмотра решения, если оно влечет юридические последствия либо способно повлиять на его права и законные интересы.

Аналогичные гарантии содержатся и в Законе «Об искусственном интеллекте». Подпункт 4) пункта 1 статьи 16 устанавливает право пользователей получать от собственника или владельца системы искусственного интеллекта разъяснения о результатах ее деятельности,

¹⁷ UNESCO. Recommendations of the Ethics of Artificial Intelligence. UNESCO: Official web-site. [Электронный ресурс]. URL: <https://unesdoc.unesco.org/ark:/48223/pf0000381137> (дата обращения: 24.04.2026).

¹⁸ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act), and amending certain Union legislative acts, Article 86. «Right to explanation of individual decision-making». EU Artificial Intelligence Act official web-site. [Электронный ресурс]. URL: <https://artificialintelligenceact.eu/article/86/> (дата обращения: 29.04.2026)

¹⁹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation – GDPR). An official web-site of the European Union. [Электронный ресурс]. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679> (дата обращения: 29.04.2026)

затрагивающей его права, свободы и законные интересы, в порядке, предусмотренном пользовательским соглашением и законодательством РК.

Закон «О персональных данных и их защите» запрещает автоматизированную обработку персональных данных, в результате которой у субъекта возникают, изменяются или прекращаются права, законные интересы. Закон также обязывает оператора разъяснять субъекту порядок автоматизированной обработки данных, возможные последствия, порядок заявления возражений и способы защиты нарушенных прав. (ст. 19-1).

Особенности применения алгоритмических систем, полностью автоматизированных решений устанавливаются законодательством Республики Казахстан.

Статья 6. Безопасность человека, общества и государства при применении цифровых технологий

1. Безопасность человека, общества и государства при применении цифровых технологий является неотъемлемым элементом устойчивого функционирования цифровой среды.

2. Государство принимает меры по предупреждению и снижению рисков негативного воздействия и применения цифровых технологий на права, свободы и законные интересы человека, общества и государства, обеспечивая их необходимость и соразмерность преследуемым целям.

1. «... информационно-коммуникационные технологии, обладая огромным потенциалом, способным содействовать развитию общества, открывают новые возможности для преступников, могут способствовать увеличению масштабов и разнообразия преступной деятельности и иметь негативные последствия для государств, предприятий и благополучия людей и общества в целом» - такое положение изложено в преамбуле Конвенции ООН против киберпреступности 2024 года²⁰. Обеспечение безопасности в цифровой среде является комплексной задачей, реализуемой как на международном, так и на национальном уровнях.

Особенность цифровой среды заключается в том, что немалая часть возникающих угроз носит трансграничный характер. Кибератаки, незаконный оборот цифровых данных, распространение вредоносного программного обеспечения, цифровое мошенничество и иные правонарушения не ограничиваются территорией одного государства. В связи с этим обеспечение безопасности цифровой среды невозможно исключительно средствами национального законодательства и требует развития международного сотрудничества.

Общее видение и стратегические ориентиры в сфере безопасности цифровой среды формируются рядом международных актов, определяющих задачи безопасного и устойчивого использования технологий, защиту прав человека, борьбу с киберпреступностью, а также развитие механизмов международного взаимодействия.

Статьей 103 Цифрового кодекса определено, что одним из основных направлений международного сотрудничества Республики Казахстан в сфере цифровизации является борьба с киберугрозами и

²⁰ Конвенция Организации Объединенных Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям. Официальный сайт Организации Объединенных Наций. [Электронный ресурс]. URL: <https://www.un.org/ru/documents/treaty/A-RES-79-243> (дата обращения: 11.06.2026)

киберпреступностью. На момент подготовки комментария в стадии ратификации находится Конвенция Совета Европы о киберпреступности (Будапештская конвенция)²¹, приглашение к присоединению к которой Казахстан получил в 2023 году.

В 2024 году ООН принята Конвенция против киберпреступности, направленная на укрепление сотрудничества государств в борьбе с преступлениями в сфере информационно-коммуникационных технологий и повышение глобального уровня кибербезопасности. Документ подписан Республикой Казахстан в октябре 2025 года, но на момент подготовки настоящего комментария не ратифицирован.

Указанные международные акты формируют единые подходы к криминализации деяний в цифровой среде, устанавливают требования к государствам определить соразмерные санкции за такие деяния, а также закрепляют процедуры быстрого взаимодействия государств для трансграничных расследований киберпреступлений. Ратификация конвенций предполагает последующую имплементацию соответствующих положений в казахстанское законодательство.

В 2018 году Казахстан ратифицировал Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности²², положения которого имеют прямое действие в отношениях Казахстана с другими странами СНГ при проведении скоординированных действий, направленных на обеспечение информационной безопасности.

Таким образом, международно-правовое регулирование определяет для Казахстана не только правовые ориентиры в сфере обеспечения безопасности цифровой среды, но и конкретные обязательства по гармонизации национального законодательства.

2. Пункт 1 статьи 6 Цифрового кодекса определяет безопасность как неотъемлемый элемент устойчивого функционирования цифровой среды, при этом выделяя разные уровни ее обеспечения: безопасность государства, общества и человека.

Такой подход отражает современное понимание безопасности в цифровой среде. Традиционные подходы к безопасности акцентируются в

²¹ Конвенция о компьютерных преступлениях (Конвенция Совета Европы о киберпреступности, Convention on Cybercrime CETS № 185) (Будапешт, 23 ноября 2001 года). Информационно-правовая система нормативных правовых актов Республики Казахстан. [Электронный ресурс]. URL: https://prg.kz/document/?doc_id=30170556 (дата обращения: 11.06.2026)

²² Закон РК от 3 мая 2018 года № 150-VI ЗРК «О ратификации Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности». Информационно-правовая система нормативных правовых актов Республики Казахстан. [Электронный ресурс]. URL: <https://adilet.zan.kz/rus/docs/Z1800000150> (дата обращения: 11.06.2026)

основном на защиту государства и общественного порядка. В цифровой среде угрозы могут быть направлены на государственную инфраструктуру, общественные процессы и права конкретного человека.

Например, утечка персональных данных может затронуть права и законные интересы миллионов граждан, создать риски для функционирования государственных информационных систем. Аналогичным образом нарушение объектов цифровой инфраструктуры способно повлиять как на национальную безопасность государства, так и на реализацию гражданами своих прав и законных интересов.

В этой связи безопасность человека, общества и государства следует рассматривать как взаимосвязанные элементы единой системы.

Как уже отмечалось, на уровне международного сотрудничества государства обязаны взаимодействовать в выявлении и пресечении киберпреступлений, применению международного права в сфере кибербезопасности, а также имплементировать в национальное законодательство стандарты безопасности.

На уровне внутренней политики государства формируется система требований к безопасности цифровой среды, определяется структура и распределение компетенций между государственными органами по обеспечению безопасности национальных интересов, предотвращения киберугроз в отношении данных и информации, содержащихся в государственных системах, и обеспечения цифрового суверенитета Республики Казахстан.

Отношения в цифровой среде, затрагивающие вопросы национальной безопасности, регулируются Законом «О национальной безопасности». В соответствии с подпунктом 5) статьи 4 информационная безопасность, являющаяся видом национальной безопасности, определена как *«состояние защищенности информационного пространства Республики Казахстан, а также прав и интересов человека и гражданина, общества и государства в информационной сфере от реальных и потенциальных угроз, при котором обеспечивается устойчивое развитие и информационная независимость страны»*.

Данное положение во многом перекликается с положениями статьи 6 Цифрового кодекса. Оба законодательных акта рассматривают безопасность не только как состояние защищенности от угроз, но и как необходимое условие устойчивого развития соответствующей сферы общественных отношений. В этом проявляется общий подход казахстанского законодательства, согласно которому развитие цифровой среды невозможно без обеспечения надлежащего уровня безопасности.

Статьей 23 Закона предусматривает, что информационная безопасность обеспечивается решениями и действиями государственных органов, организаций, должностных лиц, направленными на поддержание и развитие эффективной системы защиты цифровых ресурсов, цифровых систем и инфраструктуры связи, в которых циркулируют сведения, составляющие государственную, коммерческую и иную защищаемую законом тайну.

Дополнительно статья 5 Закона устанавливает запрет на принятие решений и совершение действий, противоречащих национальным интересам вхождения Казахстана в мировую систему связи и цифровой среды; обеспечения и повышения уровня защиты цифровых ресурсов, цифровых систем и инфраструктуры связи Республики Казахстан.

Таким образом, положения Цифрового кодекса и Закона «О национальной безопасности» формируют взаимосвязанную систему правового регулирования безопасности цифровой среды как составляющей части национальной безопасности.

3. Подпункт 1) статьи 4 Закона «О национальной безопасности» определяет общественную безопасность как *«состояние защищенности жизни, здоровья и благополучия граждан, духовно-нравственных ценностей казахстанского общества и системы социального обеспечения от реальных и потенциальных угроз, при котором обеспечивается целостность общества и его стабильность»*.

Применительно к цифровой среде понятие общественной безопасности приобретает новое содержание. Современные цифровые технологии влияют на общественные и политические процессы, экономику, формирование общественного мнения. Соответственно, объектами правовой охраны становятся цифровые данные и инфраструктура, доверие к цифровой среде, возможность безопасного использования цифровых технологий обществом в целом.

Особенность общественной безопасности в цифровой среде заключается в том, что возникающие угрозы способны одновременно затрагивать интересы большого числа лиц и быстро распространяться независимо от государственных границ. В этой связи **обеспечение общественной безопасности в цифровой среде направлено не только на противодействие кибернарушений, а на создание условий для безопасного и устойчивого развития цифровой среды.**

4. Цифровой кодекс предусматривает ряд требований и мер по обеспечению общественной безопасности в цифровой среде, включающий: установление требований к информационной безопасности цифровых объектов (ст. 27, 32, 33, 97), обеспечение безопасности хранения государственных цифровых ресурсов, размещенных на платформе

«цифрового правительства» и в цифровой инфраструктуре «цифрового правительства» (ст. 74); обеспечение защиты цифровых данных (ст. 98), обязательность соблюдения требований безопасности при цифровой аутентификации (ст. 46), а также механизмы государственного контроля в сфере цифровой безопасности (ст. 96).

Одной из ключевых составляющих безопасности в цифровой среде является кибербезопасность – состояние защищенности цифровых объектов от нарушения их конфиденциальности, целостности и доступности. Общие положения и технические требования в данной сфере определены Законом «О кибербезопасности», подзаконными актами уполномоченного органа и документами технического регулирования.

Специальные требования по обеспечению безопасности в цифровой среде определены Законами «О персональных данных и их защите», «О связи».

Меры по обеспечению безопасности функционирования онлайн-платформ, в том числе посредством предотвращения размещения противоправного контента, установлены Законом «Об онлайн-платформах и онлайн-рекламе». Его положения направлены на снижение рисков распространения незаконной информации, цифрового мошенничества, манипулирования общественным мнением и иных угроз общественной безопасности.

Дополнительное значение для обеспечения безопасности в цифровой среде имеют положения Закона «Об искусственном интеллекте», которым предусмотрен комплекс мер обеспечения безопасности при разработке и использовании систем искусственного интеллекта. К таким мерам относятся: классификация систем искусственного интеллекта по уровням риска, установление специальных требований к высокорисковым системам, обеспечение человеческого контроля за функционированием искусственного интеллекта, защита персональных данных и информационной безопасности, проведение оценки соответствия и аудита систем искусственного интеллекта и пр.

Основываясь на положениях Закона «О национальной безопасности» и положениях иных законодательных актов Республики Казахстан, регулирующих вопросы безопасности в цифровой среде, можно сделать вывод, что общественная безопасность в цифровой среде обеспечивается системой правовых, организационных и технических мер, реализуемых государственными органами, организациями, должностными лицами и гражданами. Такие меры направлены на защиту прав и свобод человека в цифровой среде личной безопасности граждан, их прав и свобод в цифровой среде; пресечение киберпреступности, обеспечение устойчивого функционирования цифровой инфраструктуры, защиту персональных

данных и иным угрозам, способным причинить вред личности, обществу и государству.

Таким образом, можно сделать вывод, что общественная безопасность в цифровой среде представляет собой не только состояние защищенности от существующих угроз, но и систему мер, реализуемых всеми субъектами цифровой среды, направленных на обеспечение ее устойчивости и создание условий для безопасного использования цифровых технологий.

При этом действующее законодательство Республики Казахстан предусматривает административную и уголовную ответственность за нарушение отдельных требований безопасности в цифровой среде, включая неправомерный доступ к информационным системам, незаконное использование персональных данных, распространение вредоносных программ, вмешательство в функционирование цифровой инфраструктуры и иные противоправные действия.

5. Безопасность человека в цифровой среде можно определить как состояние защищенности жизни, здоровья, личных прав, свобод и законных интересов человека от угроз, возникающих при использовании цифровых технологий.

Обеспечение безопасности человека в цифровой среде включает защиту персональных данных и обеспечение приватности, защиту от кибермошенничества и иных противоправных действий, а также в целом создание условий для безопасного использования цифровых технологий.

Как отмечалось в комментарии к статье 5 Цифрового кодекса, права, свободы и законные интересы человека являются высшей ценностью. Поэтому **безопасность человека следует рассматривать не как самостоятельную цель регулирования, а как необходимое условие реализации и защиты прав и свобод человека в цифровой среде.**

Одним из важных факторов обеспечения безопасности личности в цифровой среде является повышение уровня цифровой грамотности населения и формирование культуры кибергигиены. Организация обучающих мероприятий, информирование граждан о способах защиты персональных данных, безопасном использовании цифровых технологий способствует снижению уровня цифровых рисков.

6. Пункт 2 статьи 6 устанавливает обязанность государства принимать меры по предупреждению и снижению рисков негативного воздействия цифровых технологий на права, свободы и законные интересы человека, общества и государства.

Как было указано в комментарии к пункту 1 настоящей статьи, такие меры должны приниматься на уровне международного сотрудничества Республики Казахстан в сфере обеспечения безопасности цифровой среды,

формировании необходимой правовой базы, установления требований для разных субъектов и объектов цифровой среды, включая государственные базы данных, которая бы предотвращала возникновение рисков негативного воздействия цифровой среды, также в форме создания специальных органов в сфере защиты безопасности цифровой среды и наделения соответствующим компетенциями иных уполномоченных органов, разработке актов технического регулирования.

Особое значение имеет развитие национальной системы кибербезопасности. В соответствии с Законом Республики Казахстан «О кибербезопасности» государством формируется система организационных и технических мер, направленных на предупреждение, выявление и устранение угроз безопасности цифровых объектов и цифровой инфраструктуры.

[МЕСТО ДЛЯ АКТУАЛЬНОЙ ИНФОРМАЦИИ ПО КИБЕРЩИТУ ОТ СПЕЦИАЛИСТОВ]

7. Указание в пункте 2 статьи 6 на необходимость и соразмерность мер по предупреждению негативного влияния цифровой среды представляет собой прямое закрепление принципа соразмерности (пропорциональности). Его основная задача в контексте «цифрового» законодательства заключается в обеспечении баланса между защитой человека, общества и государства от цифровых рисков и сохранением условий для развития технологий и цифровой экономики.

Пункт 3 статьи 9 Кодекса дополнительно закрепляет необходимость обеспечения соразмерности между целями государственного регулирования и последствиями для человека и гражданина, а также интересами общества и государства.

В научной литературе принцип соразмерности рассматривается как общеправовой механизм разрешения конфликта между конкурирующими интересами и ценностями: «Соразмерность как принцип права представляет собой норму достаточно высокого уровня абстракции, которая реализуется через другие более конкретные нормы ... В содержательном плане принцип соразмерности включает в себя оценку целесообразности использования той или иной меры (установления того или иного правила), ее способности привести к желаемому результату; требование ее необходимости, т.е. отсутствие средства, предполагающего меньшие обременения, и сопоставление «веса» (значимости) конкурирующих интересов, затрагиваемых данной мерой (правилом).

При этом особая роль принципа соразмерности проявляется в том, что именно на его основе разрешаются конфликты не только между различными социальными интересами, но и между правовыми нормами и

иными принципами права. Посредством принципа соразмерности обеспечивается сбалансированность всей правовой системы»²³.

Если статьи 6 и 9 Цифрового кодекса закрепляют принцип соразмерности как общий подход к государственному регулированию цифровой среды, то отдельные нормы Кодекса конкретизируют его применительно к отдельным видам отношений.

Так, пункт 4 статьи 20 устанавливает, что приостановление функционирования или ограничения доступа пользователей к цифровым объектам допускается только в случаях и порядке, предусмотренных законами РК, и лишь в той мере, в какой это необходимо для защиты в целях защиты конституционного строя, охраны общественного порядка, прав и свобод человека, здоровья и нравственности населения. Данное положение препятствует необоснованному ограничению доступа к цифровым объектам и обеспечивает соблюдение баланса между публичными интересами и правами пользователей.

Пункт 4 статьи 29 детализирует принцип соразмерности применительно к регулированию цифровых платформ, закрепляя, что со стороны государства требования к цифровым платформам должны устанавливаться в объеме, соразмерном выполняемым функциям, степени влияния на права неопределенного круга лиц и характеру контроля над цифровыми данными, услугами, товарами или результатами взаимодействия.

Закрепление принципа соразмерности в Цифровом кодексе обусловлено тем, что правовое регулирование цифровой среды находится в стадии формирования и многие аспекты ее функционирования и взаимодействия человека с технологиями остаются недостаточно изученными и урегулированными. Соответственно, закрепление принципа соразмерности выступает гарантией того, что меры государственного регулирования должны быть направлены на снижение рисков, но при этом без необоснованного ограничения прав человека, конкуренции и технологического развития.

При этом, защита прав и свобод человека не должна приводить к неоправданному сдерживанию технологического развития. Как отмечалось в комментарии к статье 3 Цифрового кодекса, одной из задач цифрового законодательства является создание условий для цифровой трансформации и развития цифровой экономики. Следовательно, достижение баланса между безопасностью и развитием технологий является одной из ключевых

²³ Бажанов А.А. Соразмерность как принцип права. Диссертация на соискание ученой степени кандидата юридических наук. Москва. 2019. С. 151. [Электронный ресурс]. URL: <https://www.dissercat.com/content/sorazmernost-kak-printsip-prava> (дата обращения: 11.06.2026)

задач правового регулирования цифровой среды, поскольку стратегические задачи государства направлены на цифровую трансформацию и становление страны как регионального IT-хаба.

8. Основы реализации принципа соразмерности в нормотворческой и правоприменительной деятельности определены Конституцией Республики Казахстан 2026 года. Так, пункт 1 статьи 41 определяет: *«Права и свободы человека и гражданина могут быть ограничены только законами и лишь в той мере, в какой это необходимо в целях защиты основ конституционного строя, прав и свобод человека и гражданина, обеспечения национальной безопасности, охраны общественного порядка, здоровья граждан и нравственности общества».*

Указанное конституционное положение является ключевым и для регулирования цифровой среды. Как отмечалось в комментарии к статье 5 Цифрового кодекса, права и свободы человека в равной степени подлежат защите как в офлайн-, так и в цифровой среде. Следовательно, любые ограничения, связанные с использованием цифровых технологий, обработкой данных, цифровой идентификацией, применением алгоритмических систем должны соответствовать конституционным требованиям законности, необходимости и соразмерности.

Статья 14-2 Закона «О правовых актах» устанавливает прямое требование о соблюдении условия соразмерности при установлении государственного регулирования посредством принятия нормативных правовых актов: *«Защита конституционного строя, охрана общественного порядка, прав и свобод человека, здоровья и нравственности населения могут обусловить ограничение прав и свобод, если такое ограничение адекватно законно обоснованным целям и отвечает требованиям справедливости, является пропорциональным, соразмерным и необходимым в демократическом государстве для защиты конституционно значимых ценностей».* Данное положение имеет высокую значимость для цифровой среды, поскольку регулирование цифровых технологий в связи с новизной, не изученностью, перманентной трансформацией и развитием связано с широкими дискреционными полномочиями и вмешательством государственных органов.

Пункт 3 статьи 41 Конституции закрепляет перечень прав и свобод, которые не могут быть ограничены ни в каких случаях.

Статья 75 Конституции устанавливает конституционный контроль в отношении актов, которыми ограничиваются права и свободы человека: *«Законы и иные нормативные правовые акты, их отдельные положения, признанные не соответствующими Конституции, в том числе ущемляющими закрепленные Конституцией права и свободы человека и гражданина, прекращают свое действие и не подлежат применению со*

дня принятия Конституционным Судом решения или с даты, им установленной» (п. 2).

Таким образом, принцип соразмерности, закрепленный в статье 6 Цифрового кодекса, основывается на конституционных положениях и является одной из важнейших гарантий защиты прав человека от чрезмерного вмешательства государства в цифровой среде.

9. Принцип соразмерности имеет важное значение и для регулирования предпринимательской деятельности в цифровой среде. Развитие цифровых технологий требует создания благоприятных условий для инноваций и инвестиций.

Предпринимательским кодексом, регулирующим ведение предпринимательской деятельности в сфере цифровых технологий, принцип соразмерности закреплен в целом ряде положений, определяющих подходы государственного регулирования. Так, в пункте 1 статьи 9 установлено: *«Введение форм и средств государственного регулирования предпринимательства осуществляется в целях обеспечения достаточного уровня безопасности деятельности или действий (операций), максимальной эффективной защиты прав потребителей при минимальной объективно необходимой нагрузке на субъектов предпринимательства.*

В рамках государственного регулирования новые требования к субъектам частного предпринимательства могут вводиться только при условии преобладания выгод для потребителей, государства над издержками, связанными с осуществлением государственного регулирования».

Дополнительное развитие соблюдение принципа соразмерности получает в статье 81-1 Предпринимательского кодекса, устанавливающей условия формирования регуляторных требований. В качестве одного из обязательных условий указаны соразмерность и рациональность, под которыми понимается *«соответствие уровня воздействия государственного регулирования предпринимательства степени риска наступления неблагоприятных событий для охраняемых Конституцией и законами Республики Казахстан ценностей» (пп) 6).*

Для цифровой среды данный подход имеет особое значение, поскольку различные участники цифровой экономики обладают разным уровнем влияния на права пользователей и безопасность цифровой среды. Соответственно, объем регуляторных требований ко всем субъектам цифрового рынка должен соответствовать уровню создаваемых им рисков .

Такой подход соответствует принципу соразмерности, закрепленному в статье 6 Цифрового кодекса. Государственное регулирование должно быть достаточным для защиты прав и законных интересов граждан, но при

этом не создавать необоснованных препятствий для развития технологий, конкуренции и цифровой экономики.

10. Принцип соразмерности относится к числу принципов, соблюдение которых подлежит судебной оценке при рассмотрении споров, связанных с обжалованием действий и решений государственных органов и должностных лиц, принятых в рамках осуществления административных процедур.

«Чрезвычайно важным является принцип соразмерности для сферы административного усмотрения, в рамках которой административный орган имеет право принимать одно из нескольких допустимых с точки зрения закона (права) решений. В рамках принятия такого решения административный орган обязан применять принцип соразмерности»²⁴.

Применительно к цифровой среде административное усмотрение может реализовываться при принятии решений о блокировке либо ограничении доступа к цифровым ресурсам, применении мер реагирования в сфере кибербезопасности, использовании систем автоматизированного анализа и выявления нарушений и пр. В таких ситуациях принцип соразмерности требует, чтобы государственный орган выбирал ту меру воздействия, которая позволяет достичь законной цели с наименьшим ограничением прав и интересов участников отношений в цифровой среде.

Несоблюдение принципа соразмерности влечет возможность применения мер ответственности. Так, статья 11 Предпринимательского кодекса предусматривает персональную ответственность должностных лиц государственных органов за нанесение ущерба субъектам предпринимательства. Пункт 3 статьи 14 Предпринимательского кодекса закрепляет право предпринимателей на возмещение убытков, причиненных незаконными действиями или актами государственного органа. Административная ответственность в виде обжалования и отмены актов в суде установлена главами 12-15 Административного процессуального кодекса.

Таким образом, закрепление принципа соразмерности в Цифровом кодексе, а также соблюдение его в административной и судебной практике выступает ключевым способом ограничения чрезмерного вмешательства государства в цифровую среду и обеспечения баланса между защитой публичных интересов, развитием цифровых технологий и соблюдением прав и свобод человека. Практическое значение данного принципа заключается в том, что любые меры государственного регулирования цифровой сферы должны оцениваться с точки зрения их законности,

²⁴ Применение принципов административных процедур и административного производства в Республике Казахстан: Практическое пособие. – Астана: Библиотека суда города Астаны, 2023. [Электронный ресурс]. URL: https://prg.kz/document/?doc_id=36559243&pos=523;147 (дата обращения: 11.06.2026).

необходимости, обоснованности и минимального ограничения прав субъектов цифровых отношений.

Статья 7. Свобода обращения цифровых данных

1. В Республике Казахстан обеспечивается свобода поиска, формирования, передачи, хранения и использования цифровых данных в пределах, установленных настоящим Кодексом и законами Республики Казахстан.

2. Ограничение доступа к цифровым данным допускается в соответствии с законами Республики Казахстан.

3. Государство содействует развитию механизма открытости, достоверности, доступности, актуальности, полноты цифровых данных, их цифровой совместимости и свободного обмена цифровыми данными.

1. Цифровые данные являются ключевым ресурсом, объектом оборота и фактором создания стоимости в цифровой экономике. В отличие от традиционной (индустриальной) экономики, основанной преимущественно на производстве и обороте материальных благ, цифровая экономика формируется вокруг процессов создания, поиска, формирования, обработки, передачи, хранения и использования данных, а также результатов их аналитической обработки.

Как отмечалось в комментарии к статье 3 Цифрового кодекса, одной из задач цифрового законодательства является создание условий для цифровой трансформации всех сфер общественных отношений. Достижение данной цели невозможно без определения правового режима цифровых данных как основного ресурса цифровой экономики.

Определение цифровых данных приведено в статье 16 Цифрового кодекса: *«Цифровыми данными является информация, предоставленная в цифровой форме и пригодная для автоматизированного и (или) аналитического сбора, хранения, обработки, использования, передачи, распространения или удаления независимо от способа ее получения и формы цифрового предоставления».*

В соответствии с положениями пункта 2 статьи 12 Цифрового кодекса, **законодатель использует функциональный подход к определению понятия цифровых данных - значение имеет не только цифровая форма информации, но и ее пригодность для автоматизированного или аналитического использования посредством цифровых технологий.**

Если информация не может быть использована для автоматизированного или аналитического сбора, хранения, обработки, использования, передачи, распространения или удаления, она не соответствует признакам цифровых данных в понимании статьи 16 Цифрового кодекса.

Кодекс определяет цифровые данные как один из основных объектов, по поводу которого складываются отношения в цифровой среде. Более того, Кодекс придает цифровым данным признаки объектов гражданского оборота, что имеет существенное значение для развития цифровой экономики в Казахстане.

В момент подготовки Комментария в казахстанском законодательстве отсутствует сформированная конструкция прав на цифровые данные как самостоятельный объект. Определение правового режима цифровых данных, оснований возникновения прав на них, особенностей распоряжения и защиты должно быть реализовано в процессе предстоящей модернизации гражданского законодательства Республики Казахстан.

Признание данных объектом гражданского оборота делает актуальным вопрос о защите данных, сформированных субъектом и представляющих коммерческий интерес, в ситуации, если такие данные не составляют коммерческую тайну или не являются объектом авторского права.

Закрепление в Цифровом кодексе правового режима цифровых данных как объекта гражданских правоотношений и принципа свободы их обращения является существенным достижением разработчиков Цифрового кодекса в части преодоления позиции государства в отношении контроля над данными.

В 2021 году Административный процедурно-процессуальный кодекс был дополнен блоком статей по управлению данными. Статьей 43-2 АППК устанавливалось: *«Собственником данных, создаваемых, накапливаемых и приобретаемых за счет бюджетных средств, а также полученных иными способами, установленными законами РК, является государство»*. Таким образом, государство создавало режим государственной собственности на любые данные, которые попали в государственные базы и ограничивало доступ к ним негосударственным лицам. Указанное положение утратило силу с принятием Цифрового кодекса.

В мировой практике и научной литературе большее распространение получили концепции управления данными (data governance) и доступа к данным (data access rights). Согласно таким подходам, данные рассматриваются не как объект права, а как ресурс, представляющий информационную ценность. Соответственно, большее внимание уделяется регулированию вопросов контроля над данными, определения условий доступа, обеспечения совместимости, безопасности и справедливого использования данных. Подобный подход отражен в актах Европейского

союза: Акте о данных (Data Act)²⁵ и Регламенте об управлении данными (Data Governance Act)²⁶.

2. Пункт 1 статьи 7 закрепляет принцип свободы поиска, формирования, передачи, хранения и использования цифровых данных. Данный принцип является одним из ключевых для развития цифровой экономики, поскольку обеспечивает возможность законного обращения данных между различными субъектами цифровой среды.

В научной литературе выражается мнение о данных как особом цифровом благе²⁷. При этом отдельные категории данных, такие как открытые данные, могут рассматриваться в качестве общественного блага, поскольку данные могут одновременно использоваться неограниченным кругом лиц, не утрачивая при этом своих свойств и ценности²⁸.

Пункт 1 статьи 7 устанавливающий принцип свободы обращения данных, следует толковать **не как неограниченную свободу доступа любых субъектов к любым данным, а как установление допустимости обращения цифровых данных и доступа к ним в предусмотренных законами пределах.**

Комментируемый принцип по своему содержанию корреспондирует с конституционной гарантией свободы информации, закрепленной пунктом 3 статьи 23 Конституции: *«Право свободно получать и распространять информацию, за исключением государственных секретов, реализуется любыми не запрещенными законом способами».*

Одновременно, признание цифровых данных объектом гражданского оборота позволяет толковать пункт 1 статьи 7 и с точки зрения фундаментального гражданско-правового принципа свободы договора.

²⁵ Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). An official web-site of the European Union. [Электронный ресурс]. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R2854> (дата обращения: 05.06.2026)

²⁶ Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). An official web-site of the European Union. [Электронный ресурс]. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868&toc=OJ:L:2022:205:TOC> (дата обращения: 05.06.2026)

²⁷ Мильков А.В., Колесникова О.Ю. Цифровые данные как объекты гражданских прав. Аграрное и земельное право. 2025. № 4. С. 312–314. [Электронный ресурс]. URL: <https://cyberleninka.ru/article/n/tsifrovye-dannye-kak-objekty-grazhdanskih-prav/viewer> (дата обращения: 05.06.2026)

²⁸ Вахитова Л.Р., Кудрявцева К.В. Переосмысление понятия общественных благ в цифровую эпоху. Научный журнал НАУ ИТМО. Серия экономика и экологический менеджмент. 2020. № 2. [Электронный ресурс]. URL: <https://cyberleninka.ru/article/n/pereosmyslenie-ponyatiya-obschestvennyh-blag-v-tsifrovuyu-epohu/viewer> (дата обращения: 05.06.2026)

Признание данных объектом гражданского оборота позволяет также сопоставить пункт 1 статьи 7 с правом на свободу предпринимательской деятельности, установленного пунктом 4 статьи 29 Конституции: *«Республика Казахстан гарантирует право на свободу предпринимательской деятельности, свободное использование своего имущества для любой законной предпринимательской деятельности»*.

Например, субъекты предпринимательства вправе передавать обезличенные данные о потребительском спросе своим контрагентам для аналитических и маркетинговых целей, если такая передача не запрещена законом и не нарушает права субъектов данных.

На этапе формирования правового регулирования отношений с цифровыми данными сложно сделать однозначные выводы о них как о классическом объекте права собственности. В отличие от традиционных объектов правоотношений данные имеют свои особые характеристики: не исчерпываются при использовании, способны многократно воспроизводиться, одновременно использоваться различными субъектами, генерировать дополнительную ценность при объединении с другими данными. В связи с этим, правовой режим данных неизбежно будет уточняться.

3. Пункты 1 и 2 статьи 7 предусматривают возможность совершения с цифровыми данными таких действий как: поиск, формирование, передача, хранение и использование. Вместе с тем, статья 16 Цифрового кодекса дополнительно указывает на сбор (автоматический и аналитический), обработку, передачу, распространение, удаление данных.

Представляется правильным привести терминологию к единообразию в целях формирования однозначного понимания, толкования и применения норм, а также системной разработки актов цифрового законодательства.

Указанный перечень действий с цифровыми данными представляет собой перечисление этапов жизненного цикла данных (data lifecycle). Данный подход широко используется в международной практике управления данными, информационной безопасности и защиты персональных данных.

Структурирование этапов жизненного цикла позволяет определить какие права и обязанности возникают у субъектов на каждом этапе обращения данных, устанавливать особые требования к обработке и защите данных, разграничивать ответственных субъектов.

4. Пункт 2 статьи 7 устанавливает общее правило, согласно которому доступ к данным может быть ограничен только в соответствии с законом. Данное положение означает, что свобода обращения данных не является абсолютной и может быть ограничена в целях защиты прав и

законных интересов других лиц, обеспечения информационной безопасности, охраны государственной тайны и иных охраняемых законом интересов.

Оборот цифровых данных может быть ограничен в целях соблюдения прав субъектов данных, требований информационной безопасности, законодательством о персональных данных, интеллектуальной собственности, банковской, коммерческой и иной охраняемой законом тайны.

Указание в пункте 2 на то, что пределы свободы обращения данных могут быть установлены на уровне Цифрового кодекса или закона, препятствует субъективному произвольному ограничению доступа к данным подзаконными актами либо решениями отдельных субъектов цифровой среды, если такие ограничения прямо не предусмотрены законодательством.

Основания ограничения доступа к данным содержатся как в самом Цифровом кодексе, так и в иных законодательных актах Республики Казахстан.

«Управление цифровыми данными, содержащими государственные секреты, служебную или конфиденциальную информацию, персональные данные и иную охраняемую законом информацией, осуществляется с учетом требований и особенностей, установленных законами Республики Казахстан» (п. 4 ст. 16). Приведенное положение устанавливает особый режим доступа к разным категориям цифровых данных.

«Цифровые данные, ставшие доступными неограниченному кругу лиц вследствие их утечки, ошибки, нарушения безопасности, неправомерного их использования, предоставления доступа к ним или иных противоправных действий, не являются открытыми данными и подлежат немедленному удалению с цифровых ресурсов». Данное правило исключает возможность легализации неправомерно полученных данных через их последующее распространение.

«Приостановление функционирования или ограничение доступа пользователей к цифровым объектам допускается в случаях и порядке, предусмотренных законами Республики Казахстан, и лишь в той мере, в какой это необходимо в целях защиты конституционного строя, охраны общественного порядка, прав и свобод человека, здоровья и нравственности населения» (п. 4 ст. 20). Данное положение детализирует принцип соразмерности ограничения прав.

Отдельное место в системе ограничений занимают права собственников и владельцев цифровых объектов. Пунктом 6 статьи 24 Цифрового кодекса предусмотрено право собственников (владельцев)

цифровых ресурсов определять условия размещения, обработки и использования цифровых данных и цифровых записей, а также доступа к ним. Такое положение соответствует правомочиям собственников (владельцев) по распоряжению принадлежащим им цифровым объектам. При этом, такие ограничения не могут устанавливаться в нарушение закона.

К примеру, собственники не могут разрешить доступ к данным, который ограничен законом, не могут позволить обработку данных, если на это есть законодательный запрет. Собственники могут установить специальные требования для доступа к данным, к примеру, требование об обязательной регистрации либо установить специальную санкцию в виде ограничения доступа за нарушение условий пользовательского соглашения.

В условиях цифровой экономики контроль над ценными массивами данных превращается в форму рыночной власти. Ограничение доступа к данным как к ресурсу может осуществляться в рамках антимонопольного регулирования. Контроль над ценными массивами данных может расцениваться как барьер входа на рынок.

5. Пункт 3 статьи 7 устанавливает положение, согласно которому государство должно предпринимать активные меры для содействия создания в цифровой среде условий для свободного оборота качественных, достоверных, совместимых цифровых данных.

Данное положение следует рассматривать как одно из направлений государственной политики в сфере цифровой трансформации. Если пункт 1 комментируемой статьи закрепляет свободу обращения данных, а пункт 2 устанавливает пределы такой свободы, то пункт 3 возлагает на государство обязанность по созданию в Казахстане условий для формирования единой экосистемы цифровых данных.

Цифровые данные выступают не только ключевым ресурсом развития цифровой экономики, но и основой для принятия управленческих решений, цифровизации государственного управления услуг, развития и внедрения технологий искусственного интеллекта.

Особое значение данная норма имеет в связи с переходом государственного управления в Казахстане к модели Data-Driven Government (государственное управление на основе данных). Основная идея такой модели заключается в том, что решения органов власти должны приниматься на основе систематического, упорядоченного сбора и анализа качественных, достоверных, полных данных о социальных, экономических и иных процессах. Такой подход позволяет органам власти основывать свои решения на объективных данных, своевременно выявлять общественно значимые проблемы, прогнозировать последствия принимаемых мер, более эффективно распределять ресурсы.

Значение качественных данных возрастает и в связи с развитием технологий искусственного интеллекта, напрямую зависящих от объема и качества данных, используемых для обучения моделей. Недостовверные, неполные или устаревшие данные могут приводить к ошибочным результатам анализа, неточным прогнозам и систематическим ошибкам при принятии решений.

Перечисленные в пункте 3 «механизмы», на развитие которых должно быть направлено государственное содействие, в целях толкования целесообразно разделить на две категории. К первой группе относятся критерии качества данных: достоверность, актуальность, полнота, доступность, цифровая совместимость. Ко второй группе относятся условия свободного обращения данных: открытость и свободный обмен данными.

В теории управления данными качество данных (data quality) рассматривается как совокупность характеристик, определяющих пригодность данных для конкретных целей использования. Ценность данных определяется не только их объемом и наличием, но и степенью пригодности.

В отношении данных, используемых в государственном управлении, Постановлением Правительства «Об утверждении требований по управлению данными» установлены следующие критерии качества данных и приведено определение каждого из критериев: точность, полнота, взаимосвязанность, сопоставимость, актуальность, уникальность, достоверность, своевременность, ясность, доступность. Данные, не соответствующие перечисленным критериям, считаются недостоверными.

Международные стандарты, включая ISO 8000 (Data Quality)²⁹, ISO/IEC 25012 (Data Quality Model)³⁰ относят к ключевым критериям качества достоверность (accuracy), полноту (completeness), актуальность (timeliness или currency), согласованность (consistency), доступность и совместимость данных. Таким образом, перечень критериев качества данных, закрепленный в пункте 3 статьи 7, соответствует общепризнанным международным подходам к оценке качества данных.

Особое значение среди критериев качества данных имеет цифровая совместимость данных. Совместимость данных предполагает использование единых технических, семантических, организационных форматов, позволяющих различным информационным системам,

²⁹ ISO 8000-1:2022. Data quality – Part 1: Overview. Geneva: ISO, 2022. [Электронный ресурс]. URL: <https://www.iso.org/obp/ui/#iso:std:iso:8000:-1:ed-1:v1:en> (дата обращения: 12.06.2026)

³⁰ ISO/IEC 25012:2008. Software engineering - Software product Quality Requirements and Evaluation (SQuaRE) – Data quality model. Geneva: ISO, 2008. [Электронный ресурс]. URL: <https://www.iso.org/obp/ui/en/#iso:std:iso-iec:25012:ed-1:v1:en> (дата обращения: 12.06.2026)

программам и участникам взаимодействия «бесшовно» обмениваться и совместно использовать данные. В международной практике данное требование относится к принципу интероперабельности (interoperability), который рассматривается как одно из ключевых условий развития цифрового государства и цифровой экономики.

Статья 8. Свобода создания, развития и применения цифровых технологий

1. Создание, развитие и применение цифровых технологий осуществляются свободно, если иное не установлено настоящим Кодексом и законами Республики Казахстан.

2. Государство создает условия для проведения научных исследований, осуществления инновационной деятельности и развития цифровых технологий.

3. Государство обеспечивает реализацию мер по повышению цифровой грамотности населения, развитию доступной инфраструктуры и ликвидации цифрового неравенства, а также равные условия развития частных инициатив и конкуренции в цифровой среде.

1. Статья 8 Цифрового кодекса закрепляет один из базовых принципов регулирования цифровой среды – свободу создания, развития и применения цифровых технологий.

Как отмечалось в комментарии к статье 3 Цифрового кодекса, одной из задач цифрового законодательства является правовое обеспечение цифровой трансформации всех сфер общественных и экономических отношений. Реализация этой задачи невозможна без создания условий для свободного развития и внедрения новых технологий.

Стратегическое значение цифровизации неоднократно подчеркивалось Главой государства, который отмечал, что цифровизация и развитие технологий должны стать базовым элементом проводимых реформ. Само принятие Цифрового кодекса в Казахстане демонстрирует значимость цифровизации как ключевого фактора экономического роста и повышения глобальной конкурентоспособности Казахстана.

Важно обратить внимание на то, что статья 8 закрепляет **не обязанность государства создавать или внедрять конкретные технологии, а свободу технологического развития как общий правовой режим**. Такой подход соответствует принципу технологической нейтральности регулирования (статья 12 Цифрового кодекса), согласно которому законодательство должно создавать благоприятные условия для развития различных технологий.

Важно отметить, что понятие «**цифровые технологии**», используемое в статье 8, и иных статьях кодекса, устанавливающих общие положения в отношении цифровых технологий, является обобщающим. Оно охватывает не только отдельные технологии, но также создаваемые на их основе цифровые продукты, сервисы, платформы, системы искусственного интеллекта, цифровые объекты и иные результаты инновационной деятельности.

На момент подготовки настоящего комментария основными стратегическими документами в Республике Казахстан в сфере развития цифровизации являются Общенациональная стратегия «Digital Qazaqstan» и Концепция цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023-2029 годы.

Как указано в Концепции: «Развитие цифровой экономики также тесно связано с развитием новых видов бизнес-моделей и продуктов, основанных на цифровых технологиях. Этими продуктами мы пользуемся на ежедневной основе – финтех, платформенные решения в перевозках, заказе еды и т.д.» Цифровые технологии становятся основой формирования и развития новых рынков, бизнес-моделей и сервисов, характерных для цифровой экономики (платформенная модель, социальная коммерция, облачные вычисления, аналитика больших данных и пр.). В этой связи, положения статьи 8 Цифрового кодекса целесообразно рассматривать во взаимосвязи с положениями Предпринимательского кодекса.

Так, принцип свободы предпринимательства закреплен в статье 5 Предпринимательского кодекса и предполагает право субъектов предпринимательства осуществлять любые не запрещенные законом виды деятельности (включая новые формы, которые создаются благодаря использованию цифровых технологий). Статья 162 закрепляет определение и основные начала конкуренции: состязательность, добросовестность, законность, соблюдение прав потребителей, которые применяются одинаковым образом, в равной мере и на равных условиях ко всем субъектам рынка независимо от организационно-правовой формы и места регистрации таких субъектов рынка.

2. Одной из технологий, регулирование которой осуществляется специальным законом, является искусственный интеллект, развитие и внедрение которого в разные секторы экономики и социальной жизни также является стратегической государственной задачей. Закон «Об искусственном интеллекте» прямо предусматривает, что установленные им основы правового регулирования направлены на обеспечение развития технологий искусственного интеллекта и стимулирование их внедрения в различных сферах в целях повышения качества жизни населения и эффективности экономики.

Например, разработчики вправе создавать и внедрять новые системы искусственного интеллекта без получения специального разрешения государства, если такая деятельность не отнесена законодательством к регулируемым или запрещенным видам деятельности.

В целях развития технологии ИИ принята Концепция развития искусственного интеллекта в Республике Казахстан, согласно которой «Со стратегической позиции Казахстан определяет искусственный интеллект в

качестве приоритетного драйвера индустриального и технологического развития национальной экономики». Предполагается, что использование технологии ИИ в работе государственного аппарата будет способствовать повышению качества государственного управления, прозрачности принимаемых решений, расширению аналитических и прогнозных компетенций.

Свобода технологического развития имеет значение и для цифровизации целых отраслей экономики и социальной жизни: MedTech – развитие цифровых решений в сфере здравоохранения; AgriTech – внедрение инноваций в агропромышленный комплекс; GreenTech – использование самых современных зеленых и энергоэффективных технологий; EdTech – развитие цифрового образования и пр.

Таким образом, принцип свободы развития и использования технологий в цифровой среде имеет комплексное правовое, технологическое, экономическое и общественное значение, поскольку обеспечивает условия для развития цифрового предпринимательства, внедрения инновационных технологических решений в государственное управление, а также для расширения возможностей использования технологий в повседневной жизни.

В правоприменительной практике соблюдение данного принципа предполагает необходимость системного толкования норм цифрового законодательства во взаимосвязи с положениями Предпринимательского кодекса, законодательства о конкуренции, инновационной деятельности и технологической политике.

В целях правоприменения соблюдение указанного принципа предполагает необходимость системного толкования норм цифрового законодательства во взаимосвязи с положениями Предпринимательского кодекса, включая раздел «Экономическая конкуренция», а также положений, регулирующих сферу инновационной деятельности.

3. Пунктом 2 статьи 8 определена задача государства по созданию условий для проведения научных исследований, осуществления инновационной деятельности и развития цифровых технологий. Реализация указанных целей напрямую зависит от гибкости регуляторной базы, государственной поддержки и стимулирования инноваций. Указанное положение соответствует уже сформированной системе мер поддержки инновационной и технологической деятельности.

Так, Предпринимательским кодексом (Глава 23) определены меры поддержки инновационной деятельности, под которой понимается *«деятельность (включая интеллектуальную, творческую, научную, научно-техническую, технологическую, промышленно-инновационную, инфокоммуникационную, организационную, финансовую и (или)*

коммерческую деятельность), направленная на создание инноваций» (п. 1 ст. 41-1).

В 2024 году в Казахстане принят Закон «О технологической политике», целью которого является формирование правовых, организационных и финансовых условий для развития науки, технологической модернизации и внедрения результатов научных исследований в экономику. Законом предусмотрены механизмы финансирования научной и научно-технической деятельности, меры стимулирования развития науки, коммерциализации результатов научно-технической деятельности.

Кроме того, в Республике Казахстан сформирована система специальных правовых и режимов, направленных на стимулирование технологического развития. К ним относятся Международный технопарк Astana Hub, специальные экономические зоны технологической направленности, индустриальные зоны, инновационные кластеры, технологические парки и регуляторные песочницы. Указанные механизмы предусматривают предоставление налоговых, административных и инфраструктурных преференций субъектам инновационной деятельности.

Для устойчивого развития цифровой среды необходима государственная поддержка в форме создания технологической и цифровой инфраструктуры, развитие сетей связи, обеспечение населения высокоскоростным интернетом, создание ЦОДов и облачной инфраструктуры. Важное значение имеет финансирование инновационных проектов, включая инструменты грантовой поддержки, венчурное финансирование, государственно-частное партнерство, а также деятельность институтов развития.

Концепцией цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023 - 2029 годы предусматривает меры, направленные на подготовку высококвалифицированных специалистов в сфере IT, поддержку экспорта технологической продукции и интеграцию национальной экономики в глобальные технологические цепочки. В совокупности указанные меры направлены на повышение технологической конкурентоспособности государства, обеспечение цифровой трансформации экономики и формирование благоприятной среды для свободного развития и использования технологий.

4. Как отмечалось в комментарии к статье 5 Цифрового кодекса, свобода развития технологий не является абсолютной. Развитие и применение технологий, включая искусственный интеллект, должно осуществляться с соблюдением прав и свобод человека, требований безопасности и принципов цифровой этики.

Пункт 1 статьи 8 определяет возможность ограничения создания, развития и использования цифровых технологий только на уровне Цифрового кодекса и законов Республики Казахстан. Приведем некоторые положения Цифрового кодекса и отдельных законов Республики Казахстан, которыми установлены разного рода ограничения и запреты.

Цифровым кодексом установлены, в частности, следующие случаи ограничения свободного использования технологий:

1) алгоритмические и автоматизированные решения, затрагивающие права, свободы и законные интересы человека в цифровой среде, применяются с соблюдением прозрачности, недискриминации и возможности контроля со стороны субъекта цифровой среды (п. 3 ст. 5);

2) создание, развитие и применение цифровых технологий осуществляются с соблюдением принципов уважения прав и достоинства человека, недопустимости дискриминации, справедливости, добросовестности, прозрачности и ответственности (п. 1 ст. 13);

3) приостановление функционирования или ограничение доступа пользователей к цифровым объектам допускается в случаях и порядке, предусмотренных законами РК, и лишь в той мере, в какой это необходимо в целях защиты конституционного строя, охраны общественного порядка, прав и свобод человека, здоровья и нравственности населения (п. 4 ст. 20);

4) никто не может быть принужден к цифровой идентификации, за исключением случаев, когда такая обязанность прямо предусмотрена законами Республики Казахстан.

Отдельные ограничения закреплены и в иных законодательных актах.

Так, статьей 89 Налогового кодекса предусмотрена возможность блокировки интернет-ресурса в случаях неисполнения уведомления о постановке на регистрационный учет в налоговом органе и уведомления о расходах по результатам камерального контроля.

Статьи 53 и 54 Закона «О кибербезопасности» устанавливают порядок к защите цифровых объектов – комплекса правовых, организационных и технических мероприятий, направленных на сохранность цифровых объектов, предотвращение неправомерного или непреднамеренного доступа воздействия на них. К таким несанкционированным или непреднамеренными действиями в том числе относится блокирование цифровых ресурсов и объектов цифровой инфраструктуры, в виде действия, приводящих к ограничению и закрытию доступа к ним.

Законом «Об искусственном интеллекте» предусмотрен ряд оснований для возможного ограничения использования технологии ИИ. Статья 10 устанавливает, что эксплуатация систем искусственного интеллекта

возможна при соблюдении требований защиты данных и конфиденциальности, исключая неправомерный сбор, хранение и распространение персональных данных. Статья 17 запрещает создание и эксплуатацию отдельных видов систем ИИ.

Законом «Об онлайн-платформах и онлайн-рекламе» прямо установлено основание для ограничения деятельности онлайн-платформ на территории Республики Казахстан уполномоченным органом в случае несоблюдения законных требований к деятельности онлайн-платформ (ст. 24).

Анализ приведенных положений позволяет сделать вывод о том, что ограничение принципа свободы создания, развития и использования технологий может быть установлено в законах как в установлении обязательных требований к разработке и эксплуатации цифровых технологий и цифровых объектов, так и в применении ограничительных мер государственного воздействия: ограничение доступа, блокировку, запрет эксплуатации или установление специальных режимов контроля и безопасности. Такие ограничения могут иметь технологический, организационный, этический или правозащитный характер и быть направлены на обеспечение национальной и информационной безопасности, защиту прав граждан и общественных интересов.

3. Пункт 3 статьи 8 Цифрового кодекса предусматривает обязанность государства принимать меры, направленные на повышение цифровой грамотности населения.

Осмысленное пользование цифровыми объектами и технологиями является важным фактором безопасного и устойчивого функционирования цифровой среды в целом. Цифровая грамотность становится необходимым условием реализации прав граждан, получения государственных услуг, пользования цифровыми сервисами, а также защиты персональных данных и информационной безопасности.

Концепция цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023-2029 годы в качестве одного из целевых индикаторов предусматривает повышение уровня кибергигиены населения как базовых навыков поведения, направленных на безопасное использование технологий.

Действующее законодательство Республики Казахстан не рассматривает цифровую грамотность и соблюдение требований кибергигиены как самостоятельную обязанность пользователей в цифровой среде. Однако, отдельные положения Цифрового кодекса устанавливают косвенное требование для пользователей цифровых объектов ознакомиться с информацией об условиях использования цифровых объектов,

определенной законодательством и собственником объекта, а также действовать добросовестно (п. 3 ст. 39).

В перспективе развития цифровой среды, особенно в аспекте пользования автоматизированными сервисами, может потребоваться более детальное нормативное закрепление обязанности пользователей по соблюдению базовых требований цифровой безопасности.

Статья 9. Баланс частных и публичных интересов

1. Регулирование общественных отношений в цифровой среде осуществляется с соблюдением баланса между частными и публичными интересами.

2. Реализация публичных интересов не должна приводить к необоснованному ограничению прав частных лиц.

3. При осуществлении государственного регулирования обеспечивается соразмерность между его целями и последствиями для человека и гражданина, интересами общества и государства.

4. Государственные органы и организации обеспечивают прозрачность, открытость и мотивированность решений, принимаемых с использованием цифровых технологий.

1. Принципы правового регулирования, определенные Цифровым кодексом, представляют взаимосвязанную и взаимодополняющую систему норм, применимых к разным аспектам функционирования цифровой среды.

Принцип баланса частных и публичных интересов, закрепленный в статье 9 Цифрового кодекса, также не является изолированным, а развивает и детализирует общий подход к ограничению участия государства в цифровой среде. Положения статьи 9 целесообразно рассматривать и анализировать во взаимосвязи со принципами, установленными статьями 5, 6 и 8 Цифрового кодекса.

Принцип баланса частных и публичных интересов является межотраслевым принципом, значимость которого возросла в связи с развитием цифровой экономики и необходимости разработки гибкого правового регулирования отношений в цифровой среде. **Цифровое право, находясь в стадии формирования, представляет собой совокупность публично-правовых и частноправовых норм, что предопределяет важность соблюдения принципа баланса интересов как в правотворческой, так и в правоприменительной практике.**

Важность соблюдения баланса публичных и частных интересов обоснована тем, что интересы государства, общества, бизнеса и частных лиц могут быть взаимосвязанными, а могут и не совпадать. При этом, в публичных правоотношениях у государства есть возможность расширить свои компетенции, создать особые условия, установить специальные требования и пр., при этом ограничив интересы частных лиц.

Правовая суть и содержание «публичного интереса» является предметом дискуссий со времен римских юристов. В теории имеется много научных размышлений как над общим понятием публичного интереса, так и над его особенностями в разных отраслях права (налоговом, бюджетном,

экологическом и др.). В теории выделяются различные классификации публичного интереса: по субъектам (государственные интересы, общественные интересы, интересы отдельных социальных групп), по сферам жизни (политические, экономические, социальные). особенностям публичного интереса в публично-правовых и частноправовых отраслях (в правоприменительной практике, в гражданских правоотношениях, правовом регулировании предпринимательской деятельности).

При этом баланс публичных и частных интересов не означает их равенства в каждом конкретном случае. В отдельных ситуациях защита публичного интереса может требовать ограничения отдельных прав и интересов участников цифровой среды. Однако такие ограничения возможны только на основании закона, должны преследовать легитимную цель и соответствовать требованиям необходимости и соразмерности.

Так, установление требований по хранению отдельных категорий данных на территории Республики Казахстан может ограничивать свободу предпринимательской деятельности собственников (владельцев) цифровых объектов, однако это может быть оправдано необходимостью защиты национальной безопасности и публичных интересов.

К публичным интересам в цифровой среде могут быть отнесены: обеспечение информационной и кибербезопасности, защита и устойчивое функционирование цифровой инфраструктуры, предотвращение кибератак и иных цифровых угроз, обеспечение функционирования критически важных цифровых объектов, защита прав и безопасности пользователей цифровой среды, охрана общественного порядка и нравственности, а также обеспечение цифрового суверенитета Республики Казахстан.

2. Пункт 1 комментируемой статьи адресован законодателю и регуляторам (государственным и профессиональным саморегулируемым организациям), осуществляющим полномочия формирования правил поведения, контроля их соблюдения и юридически обоснованного принуждения к их соблюдению субъектами цифровой среды.

В данном случае понятие «публичный интерес» следует понимать в соответствии общепринятым значением, признанным в экономически развитых демократических правовых порядках, как согласовано, к примеру, в документах Организации Экономического Сотрудничества и Развития (ОЭСР).³¹

Так, если частный интерес (*private interest*) означает, в широком понимании этого термина, любой (в первую очередь, правомерный)

³¹ OECD (2026), Recommendation of the Council on OECD Guidelines for Managing Conflict of Interest in the Public Sector, OECD/LEGAL/0316; OECD (2017), Preventing Policy Capture: Integrity in Public Decision Making, OECD. Public Governance Reviews. OECD Publishing, Paris. DOI: 10.1787/9789264065239-en. [Электронный ресурс]. URL: <http://dx.doi.org/10.1787/9789264065239-en> (дата обращения: 13.06.2026)

интерес отдельного участника сферы общественных отношений в получении им прямых и косвенных выгод, то публичный интерес (*public interest*) – это потребность подавляющего большинства заинтересованных лиц в рамках данного правового порядка / юрисдикции в приемлемом уровне качества каждодневной жизни граждан, в коллективном благополучии общества, в обеспечении честности и доверия при всех существующих формах социального взаимодействия. Причем, обеспечение соблюдения публичного интереса (служение публичному интересу) признается миссией правительств и государственных учреждений.

Таким образом, не следует смешивать публичный интерес с интересами государственного аппарата, а, тем более, с интересами отдельных должностных лиц государства (какую бы высокую должность они ни занимали): согласно ГК, государство является равноправным с гражданами и юридическими лицами участником гражданских отношений, включая имущественные и регулируемые ГК личные неимущественные общественные отношения в цифровой среде.

Баланс публичных и частных интересов можно определить состояние правового регулирования, при котором права, обязанности и законные интересы участников общественных отношений находятся в согласованном и соразмерном соотношении. Его обеспечение осуществляется, прежде всего, посредством законодательной и правотворческой деятельности. На стадии подготовки и принятия нормативных актов должна оцениваться их соразмерность, необходимость и возможное влияние на интересы различных участников цифровой среды. При этом государство, защищая публичные интересы, не должно выходить за пределы необходимого вмешательства.

3. Категория «публичный интерес» в аспекте обеспечения судебной защиты используется в действующем казахстанском законодательстве. Так, одним из оснований к пересмотру дел в кассационной инстанции является нарушение прав, свобод и **законных интересов неопределенного круга лиц или иных публичных интересов** (ст. 169-1 АППК; ст. 851 КОАП; ст. 438 ГПК).

В комментариях к процессуальным кодексам разъяснение о том, что относится к таким публичным интересам отсутствует, также как нет соответствующих разъяснений в нормативных постановлениях Верховного Суда РК. Исходя из редакции норм, можно сделать вывод, что законодатель под публичными интересами понимает интересы больших групп лиц, но при этом нельзя сделать однозначного вывода, что под интересами неопределенного круга лиц понимаются общественные интересы.

Для правотворческой и особенно правоприменительной практики определение категории «публичный интерес», закрепленное в

законодательстве, представляет высокую важность. Прежде всего, должно быть определено, включают ли публичные интересы общественные интересы, либо интересы представителей публичной власти.

В отсутствие устоявшегося определения, правовой природы и содержания «публичного интереса» как в доктрине, так и в законодательстве, последствием может быть слишком широкое толкование. Применительно к цифровой среде, широкое толкование публичного интереса может выражаться в избыточном ограничении и модерации контента цифровых платформ, излишних требованиях о прозрачности и подотчетности деятельности цифровых объектов, приоритетах развития инфраструктурных объектов и пр.

4. Пунктом 2 статьи 9 устанавливается, что реализация публичных интересов не должна приводить к необоснованному ограничению прав частных лиц.

Пункт 2 комментируемой статьи следует понимать как: (i) адресованный государственному аппарату и негосударственным регуляторам отношений, складывающихся в цифровой, а также (ii) предупреждающий их от того, чтобы ограничивать права субъектов цифровой среды (государственных и негосударственных) осуществлением действий в узковедомственных интересах или интересах саморегулируемой организации.

Однако, положения этого пункта не должны препятствовать ограничению прав отдельных частных лиц (включая само государство, то есть его государственный аппарат), если этого требует охрана или соблюдение публичного интереса (public interest) в том его понимании, как изложено в пункте 1 выше.

5. Пункт 3 статьи 9 Цифрового кодекса устанавливает: *«При осуществлении государственного регулирования обеспечивается соразмерность между его целями и последствиями для человека и гражданина, интересами общества и государства».*

Данное положение дополняет пункты 1 и 2 комментируемой статьи, которые устанавливают принцип баланса частных и публичных интересов в цифровой среде. Пункт 3 определяет механизм достижения такого баланса путем соблюдения требований соразмерности.

Как уже отмечалось в комментарии к статье 6 Цифрового кодекса, принцип соразмерности определяет, чтобы меры государственного регулирования были направлены на достижение законной цели, являлись необходимыми для ее достижения и не создавали чрезмерных ограничений прав, свобод и законных интересов участников отношений в цифровой среде.

В контексте комментируемой статьи значение требования соразмерности заключается в том, что государственное регулирование цифровой среды не может обосновываться исключительно на достижении публичных целей. Одновременно должны учитываться последствия принимаемых решений для граждан, субъектов предпринимательства, развития технологий и цифровой экономики в целом.

Пункт 3 статьи 9 закрепляет принцип соразмерности как один из основных критериев оценки допустимости государственного вмешательства в цифровую среду. Более подробно вопросы реализации принципа соразмерности в правотворческой и правоприменительной практике рассмотрены в комментарии к статье 6 Цифрового кодекса.

6. Пункт 4 статьи 9 определяет: *«государственные органы и организации обеспечивают прозрачность, открытость и мотивированность решений, принимаемых с использованием цифровых технологий»*.

Данное положение является одной из гарантий соблюдения баланса частных и публичных интересов в цифровой среде. Если государственным органом решение принимается с использованием цифровых технологий и затрагивает права и законные интересы конкретного лица, то такое лицо должно иметь возможность понять основания принятия такого решения и при необходимости обжаловать его.

В этой связи пункт 4 статьи 9 следует рассматривать во взаимосвязи с пунктом 3 статьи 5 Цифрового кодекса, предусматривающим общее требование прозрачности и возможности контроля алгоритмических решений. а также со статьей 43 Кодекса, закрепляющей права субъектов в отношении полностью автоматизированных решений.

Статья 10. Доступность и инклюзивность цифровой среды

1. Государство обеспечивает равный доступ граждан к цифровым технологиям, продуктам, услугам и возможностям в цифровой среде.

2. Цифровые объекты, для которых требования по доступности установлены законодательством Республики Казахстан, разрабатываются и используются с учетом доступности для лиц с инвалидностью, а также лиц с нарушениями зрения, слуха, речи и другими функциональными ограничениями и лиц, относящихся к маломобильным группам населения.

1. Статья 10 Цифрового кодекса отражает международные обязательства Республики Казахстан и сформировавшийся в международном праве подход, согласно которому государство должно создавать условия для доступа граждан к сети Интернет и другим цифровым благам. Несмотря на отсутствие международного договора, в котором бы напрямую было закреплено право на доступ к Интернету, такое право рассматривается как необходимое условие реализации ряда фундаментальных прав и свобод человека, включая свободу выражения мнений, право на получение информации, право на образование и другие.

В казахстанской правовой доктрине еще предстоит выработать единый подход к содержанию данного права: определить понятие доступа, его юридическую природу, перечень благ для доступа, пределы и основания ограничения доступа, а также его место в системе прав человека.

Право на доступ к цифровой среде не следует понимать исключительно как доступ к сети Интернет. В условиях цифровизации всех сфер социальной жизни, такое право предполагает возможность пользования государственными цифровыми сервисами, получать финансовые услуги, реализовывать право на образование и труд и в целом полноценно участвовать в общественной жизни.

Международные подходы к обеспечению цифровой доступности закреплены в Рекомендации ЮНЕСКО о поощрении и использовании многоязычия и универсальном доступе к киберпространству (2003 г.), докладе Специального докладчика ООН по вопросу о поощрении и защите права на свободу мнений и их свободное выражение (А/НRC/17/27, 2011 г.), а также в резолюциях Совета ООН по правам человека «Поощрение, защита и осуществление прав человека в Интернете». В указанных документах подчеркивается, что права человека должны в равной степени защищаться как в офлайн-, так и в онлайн-среде, а государства должны содействовать расширению доступа к сети Интернет.

С учетом участия Казахстана в деятельности Совета ООН по правам человека и принимаемых обязательств, **обязанность государства**

обеспечить доступ к Интернету в контексте комментируемой статьи 10 должна рассматриваться как неотъемлемое условие реализации права человека и предотвращение цифрового неравенства.

Вместе с тем, закрепление принципа цифровой доступности на уровне Цифрового кодекса предполагает, что государство должно обеспечить наличие цифровой инфраструктуры, покрытие сетью Интернет, доступной стоимости услуг и достаточное качество соединения.

По состоянию на январь 2026 года 93,4% населения Казахстана имеют доступ к сети Интернет, что позволяет большинству граждан пользоваться государственными цифровыми ресурсами и услугами. Вместе с тем наличие доступа к Интернету само по себе не означает обеспечение повсеместного равного доступа. Для этого необходимы качественная связь, доступность цифровых устройств и достаточный уровень цифровой грамотности населения.

2. Основная гарантия, закрепленная в статье 10, заключается именно в обеспечении гражданам равного доступа к цифровой среде. Такое равенство предполагает:

- 1) обеспечение общего недискриминационного доступа по любым признакам – полу возрасту, этнической принадлежности, языку, степени владения навыками пользования технологиями и пр.
- 2) создание специальных условий для доступа для лиц с инвалидностью.

При этом, обязанность государства обеспечить равный доступ граждан к цифровой среде не означает полное отсутствие ограничений доступа. Установленный в статье 10 принцип заключается в том, что на уровне законодательства не могут быть закреплены дискриминационные условия для доступа.

Ограничения доступа допускаются только в случаях и порядке, предусмотренных законодательством Республики Казахстан, и должны соответствовать конституционным принципам законности, необходимости и соразмерности. Подробнее вопросы допустимых ограничений прав в цифровой среде рассмотрены в комментариях к статьям 5 и 6 Цифрового кодекса.

Важно, что ограничения могут быть закреплены только на уровне законов, а не законодательства, что усиливает уровень защиты права граждан на равный доступ к цифровой среде и невозможность ограничения такого права на уровне подзаконных актов при отсутствии закрепленного законного обоснования.

Одновременно доступ к отдельным цифровым объектам может ограничиваться их собственниками (владельцами) посредством требований о регистрации, аутентификации или соблюдении правил пользования такими объектами. Такие ограничения допускаются, если они не противоречат законодательству и применяются одинаково ко всем пользователям соответствующей категории.

Например, интернет-магазины обязаны ограничивать возможность приобретения алкогольной продукции лицами, не достигшими 21 года. Ограничения на пользование Интернетом для осужденных предусмотрены Уголовно-исполнительным кодексом Республики Казахстан (ст. 104).

Принцип равного доступа к цифровой среде не может рассматриваться как норма, в соответствии с которой исключается ограничение доступа в форме блокировки аккаунта конкретного пользователя в случаях совершения им нарушений законодательства или правил, установленных собственниками (владельцами) таких ресурсов.

Принцип равного доступа к цифровой среде не исключает возможность ограничения доступа конкретного пользователя к цифровому объекту в случае нарушения им законодательства, пользовательского соглашения или обязательных правил использования цифрового объекта.

1. Пункт 2 статьи 10 конкретизирует принцип доступности цифровой среды в отношении лиц с инвалидностью. Положения пункта фиксируют государственную политику в сфере инклюзии, основанную, в свою очередь, на международных обязательствах Республики Казахстан.

Правовой основой такой политики являются международные обязательства Республики Казахстан. Важнейшим международным актом в данной сфере является Конвенция ООН о правах инвалидов, ратифицированная Законом РК № 288-V от 20 февраля 2015 года. Конвенция предусматривает обязанность государств принимать меры по устранению барьеров, препятствующих полноценному участию лиц с инвалидностью в общественной жизни, включая доступ к информации, коммуникациям и цифровым технологиям.

Законом РК от 7 июня 2023 года № 8-VIII ЗРК ратифицирован также Факультативный протокол к Конвенции о правах инвалидов, определяющий права лиц с инвалидностью обращаться Комитет ООН по правам инвалидов с жалобами о том, что они являются жертвами нарушения этим государством-участником положений Конвенции.

Во многих странах требования о цифровой доступности закреплены на законодательном уровне. Основой таких требований

выступают Web Content Accessibility Guidelines³² – международный признанный стандарт, разработанный Консорциумом Всемирной паутины (World Wide Web Consortium), который содержит рекомендации по созданию доступных веб-сайтов и цифрового контента для людей с инвалидностью.

Подходы, основанные на стандартах WCAG и обязательные для государственных и частных цифровых ресурсов, используются в США, Европейском Союзе и ряде других стран. Целью закрепления таких стандартов является создание цифровой среды, которой люди с инвалидностью могут пользоваться наравне с другими гражданами.

Основным документом, детализирующим внедрение принципа инклюзии в государственную политику Республики Казахстан, является Концепция инклюзивной политики в Республике Казахстан на 2025 – 2030 годы.

Государственная инклюзивная политика основывается *«на признании инвалидности как социального явления с концептуальным переходом от традиционной и медицинской моделей понимания инвалидности к социально-правозащитной модели, что означает: устранение существующих барьеров, ограничивающих права людей с инвалидностью, во всех аспектах – социальном, физическом, правовом, институциональном, информационном».*

В этой связи принцип доступности, закрепленный в статье 10 Цифрового кодекса, следует рассматривать как один из способов реализации государственной инклюзивной политики в цифровой среде.

2. Комментирование пункта 2 имеет смысл начать с уточнения некоторых понятий.

«Лицо с инвалидностью – лицо, имеющее нарушение здоровья со стойким расстройством функций организма, обусловленное заболеваниями, увечьями (ранениями, травмами, контузиями), их последствиями, нарушениями, которое приводит к ограничению жизнедеятельности и необходимости его социальной защиты» (пп) 106 Социального кодекса).

Определение маломобильных групп населения закреплено в подпункте 107) Строительного кодекса Республики Казахстан: *«маломобильные группы населения – лица пожилого возраста, лица с инвалидностью, лица, испытывающие затруднения при самостоятельном передвижении, получении услуг, информации или ориентировании в пространстве, в том числе использующие детские коляски и (или) кресла-коляски».*

³² Web Content Accessibility Guidelines (WCAG) 2.1. World Wide Web Consortium official web-site. [Электронный ресурс]. URL: <https://www.w3.org/TR/WCAG21/> (дата обращения: 14.04.2026)

Перечисленные категории лиц объединены по признаку ограниченной возможности полноценного использования цифровых объектов без создания для них специальных условий. Однако, обобщающего определения для этих двух категорий в пункте 2 не закреплено.

Категории субъектов, обязанных разрабатывать цифровые объекты должны с учетом требований доступности для лиц с инвалидностью, определены статьей 42 Цифрового кодекса. Необходимо отметить, что в статье 42 указаны только лица с инвалидностью, но не указаны маломобильные группы, что, скорее всего, можно отнести к невнимательности разработчиков.

К таким субъектам относятся: государственные органы, государственные юридические лица, субъекты квазигосударственного сектора и иные лица, участвующие в оказании государственных услуг. Ключевым критерием является именно оказание государственных услуг указанными лицами, поскольку через соответствующие цифровые объекты обеспечивается реализация прав граждан на получение государственных услуг. **Важно отметить, что негосударственные лица, участвующие в оказании государственных услуг, при этом не являются участниками публично-правовых отношений и не несут обязанностей и ответственности в отношении государственных услуг, оказанных посредством цифровых ресурсов таких лиц.**

Статья 42 также устанавливает обязанность указанных субъектов учитывать единые требования к обеспечению доступности услуг в цифровой среде, при создании, развитии, модификации, эксплуатации цифровых объектов. На момент подготовки настоящего комментария действуют Единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утвержденные Постановлением Правительства РК от 20 декабря 2016 года № 832.

Помимо технических требований Единые правила устанавливают перечень отношений и видов цифровых сервисов, на которые их действие не распространяется, а, следовательно, не применяется и требование об обеспечении доступности для лиц с инвалидностью.

Едиными правилами установлено, что создание или развитие интернет-ресурса (цифрового объекта) осуществляется с учетом требований национального стандарта СТ РК 2191-2023 «Информационные технологии. Доступность веб-контента для лиц с инвалидностью», разработанного на основе актуальной версии Web Content Accessibility Guidelines (WCAG) 2.2.

3. Закрепленный статьей 10 принцип цифровой доступности следует рассматривать во взаимосвязи с другими принципами Цифрового кодекса.

Как отмечалось в комментарии к статье 5, цифровая среда должна обеспечивать реализацию прав и свобод человека. Статья 6 требует обеспечения безопасности человека, общества и государства при использовании цифровых технологий. Статья 9 Кодекса закрепляет требование о соблюдении баланса публичных и частных интересов. Следовательно, доступность цифровой среды должна обеспечиваться таким образом, чтобы одновременно гарантировать права человека, безопасность цифровой среды и соблюдение законных интересов других участников цифровых отношений.

Статья 11. Пропорциональное и обоснованное участие государства в цифровой среде

1. Государство участвует в цифровой среде в пределах, установленных настоящим Кодексом и законами Республики Казахстан.

2. Государственное участие в создании и эксплуатации цифровых ресурсов и систем допускается в целях реализации государственных функций, оказания государственных услуг, обеспечения безопасности, устойчивости и доступности цифровой инфраструктуры при соблюдении требований недопущения необоснованного вмешательства в конкурентную среду.

1. Статья 1 Цифрового кодекса определяет понятие цифровой среды как «совокупность инфраструктуры, технологий, процессов и условий для создания, обращения, хранения, передачи и использования цифровых данных и цифровых объектов, осуществления и передачи прав на них...».

По отношению к цифровой среде и к возникающим в ней отношениям государство может выступать в разных качествах. Прежде всего, как регулятор. Соответствующие компетенции государственных органов закреплены Цифровым кодексом и иными применимыми актами. Так, уполномоченный орган в сфере цифровизации осуществляет стратегические, регулятивные, реализационные и контрольные функции, разрабатывает и утверждает НПА, а также в целом определяет направления государственной политики в сфере цифровизации (ст. 14 Цифрового кодекса). Подходы, ограничивающие реализацию государством властных полномочий в цифровой среде, определены статьей 9 Цифрового кодекса «Баланс частных и публичных интересов».

Вместе с тем государство может выступать и непосредственным участником цифровых отношений. Статья 36 Цифрового кодекса устанавливает, что государственные органы и организации, являясь собственниками (владельцами) цифровых объектов или пользователями цифровых объектов, участвуя в отношениях в цифровой среде, приобретают статус субъектов цифровых отношений. В таком статусе государственные органы и организации участвуют в цифровой среде наравне с физическими и юридическими лицами.

Данный подход соответствует статье 111 Гражданского кодекса, согласно которой Республика Казахстан выступает в отношениях, регулируемых гражданским законодательством, на равных началах с иными участниками этих отношений. Статьей 1 Цифрового кодекса уточняется, что имущественные и иные гражданско-правовые отношения, возникающие в цифровой среде, регулируются гражданским

законодательством РК с учетом особенностей, установленных Цифровым кодексом (п. 2 ст. 1).

Таким образом, статья 11 Цифрового кодекса устанавливает требования к участию государства в цифровой среде не как ее регулятора, а его участие в качестве непосредственного участника цифровых отношений. Этим статья 11 отличается от статьи 9 Цифрового кодекса, которая определяет пределы осуществления государством властных полномочий в цифровой среде.

Являясь одновременно регулятором и участником рынка, государство имеет возможность создавать для себя как участника рынка, дополнительные преимущества: устанавливать требования под собственные цифровые сервисы, усложнять доступ на рынок частных субъектов, вводить обязательную интеграцию с государственными системами, устанавливать обязательное подключение и использование государственных сервисов, создавать единых операторов.

Именно риск совмещения государством функций регулятора и участника рынка является причиной закрепления в статье 11 Кодекса принципа пропорционального и обоснованного участия государства в цифровой среде.

Государство обладает доступом к административным цифровым данным, государственным информационным системам, статистическим данным, что может приводить к необоснованным возможностям в разработке цифровых сервисов.

Пункт 1 статьи 8 Цифрового кодекса устанавливает общий принцип, в соответствии с которым подобные действия государства не должны приводить к необоснованному ограничению конкуренции и частной инициативы. В этой связи положения комментируемой статьи следует рассматривать во взаимосвязи со статьей 8 Кодекса, закрепляющей свободу создания, развития и применения цифровых технологий, а также обязанность государства обеспечивать равные условия развития частных инициатив и конкуренции в цифровой среде.

2. Отдельными статьями Цифрового кодекса установлены ограничения правомочий государственных органов в отношении цифровых объектов:

1) п. 4 ст. 24 устанавливает ограничение возникновения права собственности у государства на цифровые записи как цифровые объекты: *«Цифровые записи, содержащие персональные данные и предоставленные государственным органам, используются государственными органами только на основании и в пределах, которые установлены законами Республики Казахстан, без возникновения права собственности у*

государства на такие данные, за исключением случаев, прямо предусмотренных законами Республики Казахстан»;

2) п. 5 ст. 25 определяет цели создания государственных инфраструктурных объектов, исключая возможность их использования в коммерческих целях: *«Государственные объекты цифровой инфраструктуры создаются в целях реализации государственных функций, оказания государственных услуг, защиты национальных интересов и обеспечения непрерывности государственного управления»;*

3) п. 1 ст. 34 определяет целевое использование национальных цифровых объектов, *«Национальными цифровыми объектами являются государственные цифровые объекты, статус которых установлен законами Республики Казахстан в связи с их критической значимостью для выполнения государственных функций, оказания государственных услуг либо обеспечения устойчивого функционирования цифровой архитектуры государства».*

Приведенные положения демонстрируют, что Цифровой кодекс не рассматривает государство как обычного участника цифрового рынка. Государственное участие в цифровой среде допускается лишь постольку, поскольку оно необходимо для выполнения государственных функций, оказания государственных услуг, обеспечения безопасности и устойчивого функционирования цифровой инфраструктуры.

В соответствии с общим подходом, установленным пунктом 1 статьи 11, пропорциональное государственное участие в цифровой среде должно быть обеспечено:

- закрепленной на уровне законодательства компетенцией государственных органов;
- целями и задачами участия государства в цифровой среде, установленными законодательством;
- требованиями законодательства о защите конкуренции.

3. Пункт 2 статьи 11 Цифрового кодекса прямо определяет цели вхождения государства в рынок при соблюдении требований недопущения необоснованного вмешательства в конкурентную среду: реализация государственных функций, оказание государственных услуг, обеспечение безопасности, устойчивости и доступности цифровой инфраструктуры. Перечисленные цели носят публично-правовой характер и связаны исключительно с реализацией государственных функций и обеспечением общественно значимых интересов.

Государственное участие допускается не потому, что государство является участником цифрового рынка, а потому, что на него

возложены обязанности по обеспечению функционирования государства, оказанию государственных услуг и защите общественных интересов.

Цифровая среда является частью общей экономической системы Республики Казахстан, поэтому на отношения в цифровой сфере распространяются общие принципы добросовестной конкуренции и недопустимости монополизации. В этой связи положения Цифрового кодекса должны применяться во взаимосвязи с положениями Предпринимательского кодекса о защите конкуренции.

Под конкурентной средой в соответствии со статьей 160 Предпринимательского кодекса понимается *«состязательность субъектов рынка, при которой их самостоятельные действия эффективно ограничивают возможность каждого из них односторонне воздействовать на общие условия обращения товаров на соответствующем товарном рынке»*. Применительно к комментируемой статье и участию государства в цифровой среде это означает необходимость создания условий, при которых государственные и частные субъекты выступают равными субъектами рынка без необоснованных преимуществ.

Комментируемый пункт взаимосвязан с принципом, определенным пунктом 3 статьи 8 Цифрового кодекса, которым на государство возложена обязанность обеспечивать равные условия развития частных инициатив и конкуренции в цифровой среде. Следовательно, государственное участие в цифровой среде не должно приводить к созданию преимуществ для государственных субъектов либо к установлению необоснованных ограничений для частных участников цифрового рынка.

Такие условия должны быть обеспечены, прежде всего, соразмерным регулированием, которое бы не создавало дискриминационных условий для разных категорий субъектов рынка или даже отдельных субъектов. Прозрачность решений государственных органов – также является гарантией создания равных конкурентных условий. Такая обязанность государства может также выражаться в создании и предоставлении равного доступа к инфраструктуре и цифровым решениям, равных условиях предоставления государственной поддержки, отсутствии административных барьеров.

В качестве примера прямого закрепления равных условий для государственных и частных субъектов в цифровой среде можно привести пункт 2 статьи 31 Цифрового кодекса: *«Государственные органы, государственные юридические лица, субъекты квазигосударственного сектора и субъекты частного предпринимательства, осуществляющие деятельность на территории Республики Казахстан, вправе создавать платформы обмена и оборота продуктов цифровых данных с соблюдением*

единых требований в сферах цифровизации и обеспечения кибербезопасности, а также правил функционирования платформ обмена и оборота продуктов цифровых данных, утвержденных уполномоченным органом по развитию экономики данных по согласованию с уполномоченным органом».

Ограничения участия государства в качестве участника рыночных отношений в цифровой среде закреплены не только в Цифровом кодексе, но и в иных законодательных актах Республики Казахстан.

Поскольку цифровая среда является частью экономики Республики Казахстан, на государственное участие в цифровых рынках распространяются общие ограничения, установленные Предпринимательским кодексом.

Так, статьей 21 Предпринимательского кодекса закреплены общие принципы, согласно которым государство участвует в предпринимательской деятельности в пределах, ограниченных Предпринимательским кодексом и законами. В целях развития частного предпринимательства и конкуренции государством принимаются меры, направленные на сокращение доли участия государства в предпринимательской деятельности путем ограничения создания государственных юридических лиц в сфере предпринимательства, юридических лиц с участием государства в уставном капитале.

Статья 192 Предпринимательского кодекса «Основания участия государства в предпринимательской деятельности» детализирует указанный принцип, путем определения закрытого перечня оснований государственного участия:

«1) отсутствия иной возможности обеспечения национальной безопасности, обороноспособности государства или защиты интересов общества;

2) использования и содержания стратегических объектов, находящихся в государственной собственности;

3) осуществления деятельности в сферах, отнесенных к государственной монополии;

4) отсутствия либо низкого уровня развития конкуренции на соответствующем товарном рынке».

Положения Предпринимательского кодекса устанавливают общие ограничения государственного участия в предпринимательской деятельности, то Цифровой кодекс конкретизирует их применительно к особенностям цифровой среды.

Участие государства в предпринимательской деятельности осуществляется путем:

- 1) создания государственных предприятий (государственное предпринимательство);
- 2) прямого или косвенного участия в уставных капиталах юридических лиц.

Постановлением Правительства от 28 декабря 2015 года № 1095 утвержден перечень видов деятельности, в которых допускается государственное участие.

Создание или расширение видов деятельности государственных предприятий, юридических лиц, более пятидесяти процентов акций (долей участия в уставном капитале) которых принадлежат государству, и аффилированных с ними лиц, которые будут осуществлять свою деятельность на территории Республики Казахстан, осуществляется с согласия Антимонопольного органа.

3. Конкурентное законодательство Республики Казахстан основано на принципе конкурентной нейтральности, который подразумевает равенство с точки зрения конкурентного регулирования всех участников рынка вне зависимости от формы, категории, рынка, юрисдикции и иных признаков.

Вместе с тем фактический уровень государственного участия в экономике Казахстана остается достаточно высоким, что оказывает влияние на состояние конкурентной среды.

Республика Казахстан является членом Комитета по конкуренции ОЭСР в лице Агентства по защите и развитию конкуренции РК. В 2025 году ОЭСР был проведен анализ конкурентного законодательства и правоприменительной практики, результаты которого отражены в Экспертных обзорах ОЭСР конкурентного законодательства и политики: Казахстан 2025. Относительно государственного участия в экономике Казахстана указано следующее: «В отношении государственного участия в конкурентной среде экономика Казахстана по-прежнему характеризуется высоким уровнем государственного участия. Предприятия с государственным участием широко представлены во множестве отраслей экономики, а практика создания «единых операторов» со специальными или монопольными правами усиливается. Ценовое регулирование остаётся распространённым, что свидетельствует о сохраняющихся структурных барьерах на пути перехода от плановой к полностью рыночной экономике»³³.

³³ Экспертные обзоры ОЭСР конкурентного законодательства и политики: Казахстан 2025. Ст. 10. Официальный вебсайт Организации по экономическому сотрудничеству и развитию. [Электронный

В качестве основных направлений совершенствования конкурентной политики ОЭСР рекомендует дальнейшее сокращение государственного участия в экономике, ограничение практики создания единых операторов, применение единых правил к государственным и частным субъектам, а также повышение прозрачности механизмов государственной поддержки.

4. Учитывая изложенное, положения статьи 11 Цифрового кодекса должны учитываться как при разработке нормативных правовых актов, так и при принятии решений о создании государственных цифровых объектов и цифровой инфраструктуры.

Принцип пропорционального и обоснованного участия государства означает, что государственное присутствие в цифровой среде должно быть обусловлено необходимостью реализации государственных функций, оказания государственных услуг, обеспечения безопасности и устойчивого функционирования цифровой инфраструктуры. При этом участие государства не должно приводить к необоснованному ограничению конкуренции, вытеснению частной инициативы или созданию преимуществ для государственных субъектов.

ресурсы]. URL: https://www.oecd.org/ru/publications/2025_ba40004d-ru/full-report/scope-and-application-of-kazakhstan-s-competition-law_c2ae4a81.html#back-endnote8412ddea5939 (дата обращения: 03.05.2026).

Статья 12. Технологическая нейтральность правового регулирования

1. Принцип технологической нейтральности правового регулирования предполагает равное отношение к различным цифровым технологиям.

2. Правовое регулирование отношений в цифровой среде осуществляется исходя из функциональных характеристик цифровых технологий.

3. Государство обеспечивает предсказуемость и стабильность правового регулирования при появлении новых цифровых технологий, не создавая препятствий для их развития.

1. Принцип технологической нейтральности правового регулирования в отличие от общеправовых принципов (законность, справедливость соразмерность и др.) является специальным принципом, применимым к регулированию отношений, связанных с созданием, развитием и использованием цифровых технологий.

Важно отметить, что для целей статьи 12 понятие «цифровые технологии» следует рассматривать как собирательное понятие. Под цифровыми технологиями могут пониматься как отдельные технологические решения и способы обработки данных, так и цифровые продукты, сервисы, информационные системы, платформы, программное обеспечение, алгоритмы и иные цифровые объекты, созданные с использованием таких технологий.

Использование законодателем обобщающей категории «цифровые технологии» является одним из проявлений принципа технологической нейтральности правового регулирования, поскольку позволяет распространять действие правовых норм не только на существующие, но и на будущие технологические решения.

Суть принципа технологической нейтральности правового регулирования заключается в том, что регулирование должно основываться не на особенностях конкретной технологии, а на выполняемых ею функциях и возможных последствиях ее использования. Если разные технологии решают одну и ту же задачу, к ним должны применяться единые подходы регулирования.

Принцип технологической нейтральности впервые был закреплен в 1976 году в Акте об авторском праве США (Copyright Act of 1976). Как отмечается в американской правовой доктрине: «при принятии Закона об авторском праве 1976 года Конгресс, уставший от постоянных требований пересматривать законодательство об авторском праве в связи с появлением новых технологий - таких как фонографы, кино, радио, кабельная передача

и др., полагал, что сумел защитить закон от окостенения и устаревания посредством технологически нейтральных подходов по умолчанию... »³⁴.

С конца 1990-х годов принцип технологической нейтральности стал одним из ключевых принципов регулирования цифровой среды в Европейском союзе. Он был закреплён в Директиве 2002/21/ЕС о единых основах регулирования электронных коммуникационных сетей и услуг, в преамбуле которой указывалось, что регулирование не должно предписывать использование конкретной технологии и не должно создавать преимущества для отдельных технологических решений³⁵. Впоследствии данный подход был подтверждён в Европейском кодексе электронных коммуникаций (Directive (EU) 2018/1972).

Технологически нейтральный подход используется и в современных актах, регулирующих отношения в цифровой среде: Digital Services Act и Digital Markets Act. В указанных актах регулирование выстроено в зависимости от функциональных характеристики цифровых услуг, уровня рисков и целей правовой защиты, а не вокруг конкретных технических решений.

Реализацию принципа технологической нейтральности в казахстанском законодательстве можно проследить на постепенном законодательном признании разных технологических способов подписания документов, разных технологических способах подтверждения личности, регулировании платежных услуг.

Принцип технологической нейтральности реализован и в самом Цифровом кодексе. В Кодексе преимущественно используются обобщающие категории и понятия («цифровая технология», «цифровой объект», «цифровые данные»), что позволяет избежать необходимости детального правового регулирования в отношении каждого вида объектов.

2. Пункт 2 комментируемой статьи раскрывает механизм реализации принципа технологической нейтральности правового регулирования. Если пункт 1 определяет общий подход государства к различным технологиям, то пункт 2 устанавливает, что правовое регулирование должно осуществляться исходя из функциональных характеристик цифровых технологий.

³⁴ Greenberg, B.A. (2016). Rethinking Technology Neutrality. Minnesota Law Review, 100(4), 1495–1562. [Электронный ресурс]. URL: <https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1206&context=mlr> (дата обращения: 12.05.2026)

³⁵ Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive): 2002/21/EC. An official web-site of the European Union. [Электронный ресурс]. URL: <https://eur-lex.europa.eu/eli/dir/2002/21/oj/eng> (дата обращения: 12.05.2026)

Функциональный подход означает, что для целей правового регулирования значение имеет не техническое устройство технологии, а выполняемая ею функция, характер использования и последствия ее применения. Соответственно, одинаковые по своему назначению технологии должны регулироваться по единым правилам.

Такой подход предусматривает не только равное отношение государства к различным технологиям, но и обеспечивает стабильность законодательства на перспективу в то время, как регулирование, ориентированное на конкретные технологии, может быстро устаревать, что будет требовать перманентного принятия поправок.

Практическая реализация функционального подхода проявляется, например, в регулировании электронной идентификации, цифровых платежей, государственных услуг, оказываемых в цифровом формате. Для правового регулирования значение имеет не то, какая именно технология используется, а возможность достоверного подтверждения личности, выражения воли, осуществления платежа либо результат оказания цифровой услуги.

3. Принцип технологической нейтральности направлен не только на обеспечение равного отношения к различным технологиям, но и на поддержание стабильного и предсказуемого правового регулирования изменяющихся и развивающихся цифровых технологий.

Предсказуемость регулирования имеет особое значение для цифровой экономики, поскольку разработка и внедрение новых технологий требуют долгосрочных инвестиций, соответственно все участники цифровых рынков должны иметь возможность заранее оценивать правовые последствия и риски.

Закрепленная пунктом 3 комментируемой статьи обязанность государства обеспечивать предсказуемость и стабильность правового регулирования на практике может быть реализована в следующих формах: отказа от излишне детализированного регулирования отдельных технологий; разработки норм, ориентированных на функции технологий и риски их применения; использования риск-ориентированного подхода; проведения публичных обсуждений проектов нормативных правовых актов; привлечения к разработке регулирования представителей бизнеса, научного и экспертного сообщества; учета международных стандартов и лучшей зарубежной практики; подготовки официальных разъяснений и обобщения правоприменительной практики.

4. Обязанность государства не создавать препятствий для развития технологий означает, что ограничения и обязательные требования должны быть необходимыми, обоснованными и соразмерными преследуемым целям.

Создание государством условий для беспрепятственного развития технологий предполагает: 1) отказ от внедрения необоснованных и преждевременных запретов, разрешительных процедур; 2) обоснованное и соразмерное применение разрешительных процедур; 3) создание регуляторных песочниц и пилотных проектов для апробации регулирования; 4) стимулирование интероперабельности цифровых систем и использовании открытых стандартов.

5. В связи принятием в Казахстане Закона «Об искусственном интеллекте» может возникнуть вопрос о соответствии специального регулирования конкретной технологии принципу технологической нейтральности правового регулирования.

Вместе с тем, в международной практике признается, что принцип технологической нейтральности не является абсолютным и не исключает установления специальных правил для отдельных технологий, если их применение связано с повышенными рисками для прав человека, общества или государства.

Европейские законотворцы приходят к выводу о том, что принцип технологической нейтральности в правовом регулировании искусственного интеллекта не может использоваться в качестве единственного регуляторного подхода. Так, в Регламенте Европейского союза об искусственном интеллекте (Artificial Intelligence Act)³⁶, наряду с технологически нейтральными нормами устанавливает специальные требования к системам ИИ в зависимости от уровня создаваемого ими риска. В частности, статья 5 AI Act запрещает отдельные практики применения ИИ, а статьи 6 и 8-15 вводят специальный правовой режим для высокорисковых систем искусственного интеллекта.

Применение исключительно принципа технологической нейтральности в отношении искусственного интеллекта может привести к высоким рискам злоупотреблений, поскольку данная технология создает качественно новые угрозы, связанные с автономностью принятия решений, непрозрачностью алгоритмов, масштабной обработкой данных и потенциальным воздействием на права человека.

Технология искусственного интеллекта носит далеко не вспомогательный характер, а может влиять на принятие решений, формирование социальных процессов, затрагивать реализацию прав и свобод. В связи с этим, регулирование технологии искусственного

³⁶ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). An Official website of the European Union. [Электронный ресурс]. URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng> (дата обращения: 12.06.2026)

интеллекта базируется на иных подходах, прежде всего, риск-ориентированном, основанном на оценке потенциального воздействия технологии на права и интересы человека и общества. Возможно, искусственный интеллект окажется не единственной подобной технологией.

Статья 13. Цифровая этика и социальная ответственность

1. Создание, развитие и применение цифровых технологий осуществляются с соблюдением принципов уважения прав и достоинства человека, недопустимости дискриминации, справедливости, добросовестности, прозрачности и ответственности.

2. Государство, организации и граждане участвуют в формировании и соблюдении этических стандартов поведения в цифровой среде, направленных на предотвращение дискриминации, манипуляции, злоупотребления цифровыми технологиями и иных нарушений прав, свобод и законных интересов человека, общества и государства.

1. Статья 13 Цифрового кодекса закрепляет принцип цифровой этики и социальной ответственности, который дополняет правовые механизмы регулирования отношений в цифровой среде.

Пункт 1 устанавливает: «Создание, развитие и применение цифровых технологий осуществляются с соблюдением принципов уважения прав и достоинства человека, недопустимости дискриминации, справедливости, добросовестности, прозрачности и ответственности».

В теории процесс усиления правовых норм этическими и моральными началами принято называть этизацией права. Использование этических ориентиров позволяет сделать правовое регулирование более человекоцентричным, обеспечить защиту достоинства, свободы и автономии человека, а также обеспечить доверие общества к новым технологиям и правилам их применения.

Пункт 1 статьи 13 закрепляет ценностные ориентиры, которые должны учитываться при разработке законодательства, создании и использовании цифровых технологий, а также при толковании иных норм цифрового законодательства.

Указанные в статье категории «справедливость», «добросовестность», «прозрачность», «ответственность» являются оценочными понятиями. Их включение в Кодекс обосновано тем, что многие риски цифровой среды невозможно предвидеть и заранее предотвратить путем установления ограничений и запретов.

Как и принцип технологической нейтральности, установленный статьей 12 Кодекса, закрепление этических требований направлено на формирование стабильного и универсального регулирования цифровой среды. Быстрота изменения и появления новых технологий, способов их использования, а также влияние технологий на социальную и экономическую жизнь вызывает необходимость формирования такого регулирования, которое бы определяло ключевые требования в аспекте защиты основных прав и свобод человека, интересов государства и

общества и не нуждалось в перманентном обновлении. Этические принципы и общие ценности такие как, достоинство, справедливость, добросовестность, недискриминация, неизменные вне зависимости от сферы их применения, обеспечивают стабильность регулирования.

В цифровой среде традиционные правовые и этические ценности приобретают новое содержание. Так, достоинство личности предполагает защиту от алгоритмической дискриминации и манипулирования поведением человека, справедливость требует оценки не только результатов автоматизированных решений, но и принципов работы алгоритмов, на которых такие решения основаны.

Взаимосвязь правового и этического регулирования в Цифровом кодексе и иных актах, регулирующих отношения в цифровой среде, реализуется в форме их взаимодействия. Так, к примеру, статьей 13 устанавливается этический принцип недискриминации при применении технологий. В свою очередь, статья 43 Кодекса устанавливает требование о том, что решения, принимаемые с использованием алгоритмических систем, не должны приводить к дискриминации. Принцип уважения достоинства обеспечивается запретом на создание и эксплуатацию систем искусственного интеллекта, использующих подсознательные, манипулятивные или иные методы, искажающие поведение физического лица и ограничивающие способность принимать осознанные решения или вынуждающие принимать решения, которые могут причинить вред или создать угрозу причинения вреда (ст. 17 Закона «Об искусственном интеллекте»).

В пункте 1 комментируемой статьи этические требования распространяются на три ключевых этапа взаимодействия с технологиями: разработка, развитие и применение. Соблюдение этических требований имеет значение на всех этапах жизненного цикла цифровой технологии или объекта и должно соблюдаться всеми вовлеченными субъектами: от разработчиков до пользователей.

Нужно отметить, что понятие «цифровые технологии» в контексте статьи 13 является обобщающим и включает такие понятия как цифровые объекты, сервисы, услуги и пр.

Соблюдение этических принципов должно обеспечиваться уже на этапе разработки технологии, когда закладываются основы работы алгоритмов, архитектура системы, критерии сбора данных. В Концепции развития искусственного интеллекта отдельно подчеркивается: *«Этическая безопасность (III) направлена на обеспечение справедливости и непредвзятости искусственного интеллекта, что содержит анализ данных на предмет возможных предвзятостей и разработку алгоритмов, учитывающих разнообразие и инклюзивность».*

Этические риски сохраняются и на стадии развития технологий, включая их модернизацию, масштабирование и усиление автоматизации. По мере расширения использования цифровых систем могут усиливаться дискриминационные эффекты, снижаться уровень приватности, возрастать возможности манипулирования поведением пользователей.

Применение технологий включает в себя использование технологий, включая цифровые объекты, по их назначению, а также применение технологий для решения конкретных задач. Именно на этой стадии влияние технологий на права и интересы граждан проявляется максимально, что усиливает важность соблюдения этических принципов.

2. Особое значение рассматриваемый принцип приобретает применительно к регулированию искусственного интеллекта. Технологии ИИ способны принести человечеству как огромную пользу, так и имеют риски этического порядка, которые могут поставить под угрозу культурное, социальное и биологическое разнообразие и усугублять социальное или экономическое расслоение – так отмечается в Рекомендациях об этических аспектах искусственного интеллекта, принятых ЮНЕСКО в 2021 году³⁷. Рекомендации ЮНЕСКО являются первой глобальной рамочной основой для этичного ИИ, принятой 193 государствами-членами (включая Казахстан).

Цифровой кодекс и Закон «Об искусственном интеллекте» во многом учитывают Рекомендации ЮНЕСКО. Прежде всего, закреплён человекоцентричный подход: права, свободы и законные интересы человека признаются высшей ценностью. Справедливость и отказ от дискриминации, безопасность, подконтрольность человеку и свобода воли также отражены в казахстанском законодательстве.

3. Пункт 2 комментируемой статьи определяет в качестве желаемой меры реализации подхода, установленного пунктом 1, участие государства, организаций и граждан в формировании и соблюдении этических стандартов поведения в цифровой среде. Таким образом, пункт 2 определяет, что обеспечение цифровой этики является задачей не только государства, но и всех участников цифровой среды.

Закрепление в законодательстве этических норм не может быть исключительно декларативным, а должно быть обеспечено системой контроля за их соблюдением. Рекомендациями ЮНЕСКО по этике искусственного интеллекта предусмотрен ряд мер, направленных на обеспечение соблюдения этических принципов в отношении систем

³⁷ UNESCO. Recommendation on the ethics of artificial intelligence. Paris: UNESCO, 2022. UNESCO: Official web-site. [Электронный ресурс]. URL: <https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence> (дата обращения: 08.05.2026)

искусственного интеллекта. Но такие способы могут применяться и в отношении других технологий и цифровых объектов.

Одной из ключевых инструментов названа оценка этического воздействия, которая представляет собой процедуру анализа цифровой технологии, системы ИИ, цифрового сервиса, направленную на выявление возможных рисков для прав человека, безопасности, недопущения дискриминации до начала или в процессе ее использования. Действующим казахстанским законодательством такая мера пока не предусмотрена. Однако, добросовестным и дальновидным разработчикам систем искусственного интеллекта стоит учитывать риск дискриминации пользователей по признаку пола, возраста или иных характеристик даже в случаях, когда такие требования прямо не предусмотрены специальными нормами законодательства.

Важным элементом обеспечения цифровой этики является определенный уровень прозрачности функционирования систем искусственного интеллекта, цифровых технологий, алгоритмов, рекомендательных систем. Это может предполагать обязанность разработчиков раскрывать информацию о принципах работы алгоритмов, источниках используемых данных, уровне автоматизации решений и потенциальных рисках применения технологий.

В отдельных случаях целесообразным представляется введение обязательного внешнего аудита высокорисковых систем искусственного интеллекта с участием независимых экспертов, специалистов по правам человека и представителей гражданского общества.

Со стороны государства дополнительным механизмом обеспечения цифровой этики может стать создание советов или комиссий по этике при отраслевых государственных органах. Такие институты могут разрабатывать документы рекомендательного типа, стандарты поведения, разрешать конфликтные или спорные ситуации.

Обязанность содействия соблюдения этических принципов возлагается не только на государство. Цифровая среда – это зона совместной ответственности государства, профессиональных участников цифровой среды и самих пользователей. Важную роль в этом взаимодействии играют профессиональные сообщества и объединения крупных технологических компаний посредством разработки кодексов цифровой этики, стандартов добросовестного поведения, механизмов саморегулирования. Присоединение к таким кодексам может означать принятие участниками добровольных обязательств по соблюдению этических требований.

Дополнительными мерами содействия цифровой этике могут выступать проведение независимых исследований и общественных

консультаций, обучение специалистов вопросам цифровой этики, развитие программ цифровой грамотности населения, поддержка общественного контроля, а также популяризация принципов ответственного и безопасного поведения в цифровой среде.

Важными участниками формирования этического цифрового пространства являются пользователи – граждане. Содействие соблюдению цифровой этики может выражаться в ответственном и этическом поведении в сети, уважении прав и достоинства других пользователей, недопустимости распространения недостоверной информации и дискриминационного контента.

Таким образом, статья 13 гармонично завершает систему принципов Цифрового кодекса, закрепляя ценностные ориентиры создания и использования цифровых технологий, дополняя иные принципы, определяющие права субъектов цифровой среды, безопасность, доступность данных или пределы участия государства.

II. Комментарий к статьям 24, 25, 28, 29, 30, 31, 39

РАЗДЕЛ II. ОБЪЕКТЫ ЦИФРОВОЙ СРЕДЫ

Глава 4. ЦИФРОВЫЕ ОБЪЕКТЫ

Статья 24. Цифровые ресурсы

1. Цифровой ресурс – совокупность упорядоченных цифровых данных, цифровых записей и программного обеспечения для их создания, хранения, обработки, отображения и распространения.

2. Цифровой ресурс, размещенный на цифровой инфраструктуре и идентифицируемый посредством доменного имени, адреса Интернета или иного цифрового идентификатора, признается интернет-ресурсом.

3. С учетом ограничений, установленных законами Республики Казахстан, собственник и (или) владелец цифрового ресурса вправе:

1) устанавливать порядок и условия доступа к цифровому ресурсу, а также правила пользования таким цифровым ресурсом;

2) использовать обозначения, идентификаторы и иные средства индивидуализации цифрового ресурса, не запрещенные законами Республики Казахстан;

3) защищать свои права, свободы и законные интересы от незаконного вмешательства, воздействия, блокировки, копирования, модификации, нарушения безопасности или иного неправомерного использования цифрового ресурса.

4. Собственник и (или) владелец цифрового ресурса обязаны:

1) обеспечивать сохранность, целостность, защиту и конфиденциальность цифровых данных, цифровых записей, размещенных или обрабатываемых в цифровом ресурсе;

2) соблюдать требования законодательства Республики Казахстан о персональных данных и их защите;

3) предоставлять пользователям цифрового ресурса информацию об условиях доступа, обработки цифровых данных и цифровых записей и использования его функционала.

5. Собственник и (или) владелец имеют иные права и выполняют иные обязанности, установленные законами Республики Казахстан.

6. Условия размещения, обработки и использования цифровых данных и цифровых записей в цифровых ресурсах, а также доступа к таким цифровым данным и цифровым записям определяются законодательством

Республики Казахстан, условиями публичной оферты, пользовательским соглашением или иными договорами, заключенными с пользователями цифрового ресурса.

1. Комментарий к статье, определяющей особенности правового режима цифровых ресурсов, целесообразно начать с анализа самого понятия «цифровой ресурс» и его места в системе объектов цифровой среды.

Как указано в комментарии к статье 20 «Цифровые объекты», законодатель использует функциональный подход к их классификации. Основанием для выделения отдельных категорий объектов цифровой среды является их функциональное назначение и выполняемая роль в цифровой среде. Такой подход основан на принципе технологической нейтральности правового регулирования, закрепленном в статье 12 Цифрового кодекса, согласно которому правовое регулирование отношений в цифровой среде осуществляется исходя из функциональных характеристик цифровых технологий.

В этой связи цифровой ресурс следует рассматривать как технологический объект, включающий элемент программного обеспечения, основным функциональным назначением которого является создание условий для организованного существования цифровых данных и цифровых записей, их накопления, хранения, обработки, отображения, распространения.

Цифровые ресурсы являются основой и обеспечивают функционирование всех цифровых систем, о чем подробно изложено в комментарии к статье 28 Цифрового кодекса.

Цифровые ресурсы могут быть государственными и негосударственными. Комментарии в отношении отдельных видов государственных цифровых ресурсов изложены к статьям Раздела 5 Цифрового кодекса.

Понятие «цифровой ресурс» не относится к числу устоявшихся. В международных актах и зарубежном законодательстве при определении организованных цифровых сред чаще используются такие понятия как информационные ресурсы (information resources), хранилища данных (data repositories), пространства данных (data spaces).

К цифровым ресурсам можно отнести базы данных, корпоративные информационные системы, электронные библиотеки и архивы, репозитории научных публикаций, ведомственные информационные системы.

Пунктом 3 статьи 20 Цифрового кодекса предусмотрено проведение Уполномоченным органом в сфере цифровизации систематизации

цифровых ресурсов и создание классификатора цифровых объектов, ориентируясь на который можно определить, к какому виду относится тот или иной цифровой объект.

Понятие «цифровой ресурс» заменило ранее использовавшееся в законодательстве понятие «электронный информационный ресурс». В Законе «Об информатизации» (теперь – Закон «О кибербезопасности»), отдельные положения которого утратили силу в связи с принятием Цифрового кодекса, понятие «электронный информационный ресурс» определялось как данные в электронно-цифровой форме, содержащиеся на электронном носителе и в объектах информатизации (пп) 57 ст. 1).

В Законе «Об информатизации» основной акцент был сделан на самих данных и их электронной форме. Статья 24 Цифрового кодекса определяет цифровой ресурс не только как совокупность данных, но и как организованную среду для их создания, хранения, обработки, отображения и распространения.

Важно отметить, что в определении цифрового ресурса указано на упорядоченность цифровых данных. Это означает, что цифровой ресурс представляет собой не случайный набор несвязанных между собой данных, а структурно организованную цифровую среду, которая позволяет ему функционировать.

Следует также обратить внимание, что перечисленные в определении процессы создания, хранения, обработки, отображения и распространения данных отражают не только функционал цифрового ресурса, но и основные этапы жизненного цикла данных (data lifecycle), являющихся основным содержанием цифрового ресурса.

Таким образом, исходя из изложенного, можно сделать вывод, что статья 24 определяет **цифровой ресурс как самостоятельный вид цифровых объектов, функциональной задачей которого является создание организованной среды для других видов цифровых объектов: цифровых данных и цифровых записей.**

Именно цифровые данные представляют собой основной элемент цифрового ресурса и иных цифровых объектов. С экономической и правовой точки зрения ценность цифрового ресурса определяется прежде всего объемом, качеством, актуальностью и возможностью использования содержащихся в нем данных. Соответственно, **правовой режим цифрового ресурса во многом зависит от правового режима содержащихся в нем данных и цифровых записей.**

2. Пункт 2 комментируемой статьи определяет отдельный вид цифровых ресурсов – интернет-ресурс, отличительным признаком которого является функционирование в сети Интернет.

К интернет-ресурсам относятся: веб-сайты; облачные сервисы; поисковые системы; цифровые платформы; мобильные приложения, взаимодействующие с пользователем через сеть Интернет.

Понятие «интернет-ресурс» широко используется как в законодательстве, так и в теории цифрового права и цифровизации и имеет устоявшееся значение.

Пункт 2 определяет дополнительные признаки интернет-ресурса: доменное имя, IP-адреса или иного идентификатора. Таким образом, руководствуясь принципом технологической нейтральности правового регулирования, законодатель не отождествляет понятие интернет-ресурса с веб-сайтом, что позволяет не изменять редакцию положений Кодекса в связи с возможным расширением видов организации цифровых данных в сети Интернет.

Выделение цифровых ресурсов, размещенных в открытой сети Интернет, в качестве самостоятельного вида, предполагает применение повышенных требований к информационной безопасности и кибербезопасности, поскольку повышаются риски несанкционированного доступа, вредоносного воздействия, кибератак, распространения вредоносного контента и пр.

3. Пункты 3-5 статьи 24 определяют объем прав и обязанностей собственников и владельцев цифровых ресурсов, которые следует рассматривать во взаимосвязи со статьей 38 Цифрового кодекса, устанавливающей общие права и обязанностей собственников и владельцев в отношении всех видов цифровых объектов.

Особенности правового регулирования цифровых ресурсов, принадлежащих государственным органам и организациям, определены Цифровым кодексом, Законом «О доступе к информации», подзаконными правовыми актами.

В соответствии со статьей 38 Цифрового кодекса собственники (владельцы) цифровых объектов обладают правом собственности или иными предусмотренными законодательством правами в отношении цифровых объектов, обязаны соблюдать права и законные интересы третьих лиц, принимать меры по предотвращению неправомерного доступа и несут ответственность за вред, причиненный вследствие неправомерного создания, использования или распоряжения цифровыми объектами.

Детальный комментарий относительного правового статуса собственников (владельцев) цифровых объектов как объектов гражданско-правовых отношений изложен к статьям 36, 38 Цифрового кодекса.

Пункты 3 и 4 статьи 24 устанавливают специальные права и обязанности собственников (владельцев), обусловленные спецификой

цифрового ресурса как технологического объекта, главной функциональной особенностью которого является создание и поддержание организованной среды для хранения, обработки и использования цифровых данных и цифровых записей.

4. Пунктом 3 статьи 24 установлено, что собственники (владельцы) цифровых ресурсов осуществляют принадлежащие им права с учетом ограничений, установленных законами Республики Казахстан. Такая оговорка отражает общие подходы, определенные статьями 5, 6, 7 Цифрового кодекса, согласно которым высшей ценностью в цифровой среде признаются права и свободы человека, а также устанавливается защита публичных интересов.

В отношении государственных цифровых ресурсов могут применяться положения статей 9, 10 Кодекса, а также специальные требования в отношении государственных цифровых ресурсов.

Цифровым кодексом предусмотрены следующие ограничения, которые должны соблюдаться собственниками (владельцами) цифровых ресурсов:

- *«ограничение прав, свобод и законных интересов человека в цифровой среде возможно только законами РК и лишь в мере необходимости для защиты конституционного строя, общественного порядка, прав и свобод человека, здоровья и нравственности населения»* (п. 1 ст. 5);

- *«ограничение доступа к цифровым данным допускается в соответствии с законами РК»* (п. 2 ст.7);

- *«приостановление функционирования или ограничение доступа к цифровым объектам допускается в случаях и порядке, предусмотренных законами РК»* (п. 4 ст.20);

- невозможности ограничения доступа к открытым данным (п. 1 ст. 17);

- исключение из гражданского оборота идентификационных цифровых записей (п. 3 ст. 21);

- соблюдение личных неимущественных прав, а также иных правомочий субъектов цифровых данных (п. 4 ст. 37).

Цифровым кодексом, а также отдельными законами Республики Казахстан предусмотрены ограничения относительно обработки персональных данных, а также особого режим информации с ограниченным доступом. Отдельные ограничения могут устанавливаться в целях соблюдения требований кибербезопасности.

5. Подпункт 1) пункта 3 статьи 24 закрепляет одно из основных правомочий собственников (владельцев) цифровых ресурсов – право на

управление доступом, посредством которого определяются и условия функционирования цифрового ресурса, защита содержащихся в нем данных, определение прав и обязанностей пользователей.

К условиям доступа можно отнести:

- технические требования: регистрация, цифровая аутентификация, ввод пароля, использование единого шлюза (для государственных ресурсов);
- требования к пользователям: корпоративная принадлежность, возраст, членство в сообществе, географическая локация и пр.;
- требования о присоединении к условиям пользования ресурсом;
- коммерческие условия: оплата подписки, членства.

При этом, важно понимать, что **право собственника (владельца) определять условия доступа не является абсолютным, поскольку должно реализовываться с учетом принципов свободы обращения цифровых данных и доступности цифровой среды.**

В случаях, когда цифровой ресурс содержит открытые данные либо используется для реализации публично значимых функций, пределы усмотрения собственника на определение условий доступа могут быть ограничены законодательством (ст. 17 Цифрового кодекса).

6. Подпункт 2) пункта 3 статьи 24 предоставляет собственнику (владельцу) цифрового ресурса право использовать обозначения, идентификаторы и иные средства индивидуализации цифрового ресурса, не запрещенные законами Республики Казахстан.

Необходимость закрепления такого права обусловлена тем, что цифровые ресурсы в цифровой среде должны быть индивидуализированы, чтобы можно было отличить их от других цифровых объектов.

В цифровой среде идентификатор также может выполнять не только функцию индивидуализации объекта, но и обеспечивать доступ к нему. К таким идентификаторам относятся: доменное имя; URL; API-идентификатор; адрес распределенного реестра; идентификатор приложения.

Кроме этого, индивидуализация цифрового ресурса снижает риски неправомерного использования его обозначений и идентификаторов, а также защиту связанных с ним прав на объекты интеллектуальной собственности (товарные знаки, авторский контент, дизайн, графические элементы, объекты патентных прав). Средства индивидуализации также способствуют повышению узнаваемости цифрового ресурса и продвижению связанных с ним цифровых продуктов и услуг.

Цифровые ресурсы являются объектами гражданского оборота, соответственно, требуют наделения их уникальными признаками, которые позволяют однозначно их идентифицировать в целях совершения сделок.

Кроме того, идентификация цифровых субъектов и объектов становится существенным условием установления взаимосвязей в цифровой среде.

Казахстанское законодательство не устанавливает перечень идентификаторов цифровых ресурсов, функционирующих не в сети Интернет. Таким образом, в качестве идентификатора может быть любое обозначение, не противоречащее положениям законодательства, к примеру, наименование программы, лицензионный ключ продукта, идентификатор версии, товарный знак, идентификатор разработчика и пр.

Для интернет-ресурсов средствами идентификации могут являться доменное имя, URL-адрес или иной цифровой идентификатор, позволяющий однозначно определить соответствующий ресурс в сети Интернет.

7. Подпункт 3 пункта 3 статьи 24 закрепляет право собственников (владельцев) цифровых ресурсов защищать свои права и интересы от незаконного вмешательства, воздействия, блокировки, копирования, модификации, нарушения безопасности или иного неправомерного использования цифрового ресурса.

Положения статьи 24 можно определить как специальное право на защиту своих гражданских прав, но с учетом специфики цифровых объектов. Перечисленные в подпункте 3) пункта 3 действия являются особыми видами рисков нарушения прав в отношении цифровых объектов со стороны третьих лиц.

Способами защиты в указанных случаях является, прежде всего, самозащита (без обращения в суд) собственников (владельцев), которая заключается в принятии соответствующих технологических и организационных мер, направленных на обеспечение устойчивого функционирования цифрового ресурса. К таким мерам относятся: резервное копирование данных, шифрование, разграничение прав доступа, криптографическая защита, применение антивирусных программ и др.

Защита прав собственников (владельцев) цифровых ресурсов предусматривает и защиту судебную. В частности, собственник (владелец) вправе требовать прекращения неправомерного доступа к цифровому ресурсу, удаления незаконно размещенной информации, восстановления доступа к ресурсу, пресечения действий, создающих угрозу его функционированию, возмещения убытков, компенсации вреда, а также

применения иных мер защиты, предусмотренных законодательством Республики Казахстан.

8. Пункт 4 статьи 24 устанавливает специальные обязанности собственников и владельцев цифровых ресурсов. В отличие от статьи 38 Цифрового кодекса, которая закрепляет общие обязанности собственников и владельцев всех цифровых объектов статья 24 в целом сформулирована с учетом особенностей функционального назначения цифровых ресурсов как организованной среды хранения, обработки и использования цифровых данных и цифровых записей.

Так, подпункт 3) пункта 2 статьи 38 возлагает на собственников (владельцев) цифровых объектов общую обязанность принимать меры по предотвращению неправомерного доступа, копирования, изменения или удаления цифровых данных и цифровых объектов. Статья 24 уточняет такие требования применительно к цифровым ресурсам.

Перечисленные меры соответствуют системе требований по управлению данными (data governance), которые предполагают установление правил сбора, хранения, использования, контроля качества и защиты данных на протяжении всего их жизненного цикла. Как было указано в комментарии к статье 7 Цифрового кодекса, цифровые данные являются основным ресурсом цифровой экономики и самостоятельным объектом защиты.

Цифровой ресурс является средой, в которой могут храниться, обращаться, размещаться данные разных субъектов, включая персональные данные. Обязанность, предусмотренная подпунктами 1) и 2) пункта 4 статьи 24 направлена, на охрану и защиту прав и законных интересов субъектов цифровых данных, включая персональные, установленную пунктом 4 статьи 37 Цифрового кодекса, а также положениями Цифрового кодекса, регулирующими вопросы защиты персональных данных, а также Законом «О персональных данных».

Исполнение обязанности по обеспечению сохранности, целостности и конфиденциальности цифровых данных предполагает принятие правовых, организационных и технических мер, направленных на предотвращение утраты и утечки данных, их несанкционированного изменения, уничтожения, распространения или иного неправомерного использования.

К таким мерам можно отнести: неукоснительное соблюдение требований законодательства, системы контроля доступа и ведение записей о доступе, использование средств криптографической защиты, шифрование данных, использование систем резервирования, разработка внутренних документов и определение ответственных лиц, разграничение данных по категориям (общедоступные и с ограниченным доступом), журналирование действий и др.

Требования в отношении применения разных средств защиты предусмотрены рядом международных и национальных стандартов.

При исполнении установленной подпунктом 1) пункта 4 статьи 24 Цифрового кодекса собственники (владельцы) цифрового ресурса должны учитывать особенности правового режима разных категорий обрабатываемых данных. В частности, статья 16 Цифрового кодекса предусматривает специальный порядок обращения с цифровыми данными, содержащими государственные секреты, служебную, конфиденциальную информацию, персональные данные и иную охраняемую законом информацию; статья 21 Цифрового кодекса, а также Закон «О цифровых активах» устанавливает особенности обращения цифровых записей.

Учитывая изложенное, можно сделать вывод о том, что **права собственников (владельцев) ограничены спецификой цифровых ресурсов, которые являются организованной средой для других цифровых объектов: цифровых данных и цифровых записей.**

9. Обязанность по предоставлению пользователям информации об условиях доступа к цифровому ресурсу, обработки цифровых данных и цифровых записей направлена на реализацию принципа свободного и осознанного волеизъявления человека в цифровой среде, закрепленного в пункте 2 статьи 5 Цифрового кодекса. Пользователь должен иметь возможность заранее понимать условия использования цифровым ресурсом.

Данная норма также обеспечивает реализацию прав субъектов цифровых данных, предусмотренных пунктом 4 статьи 37 Кодекса, включая право на получение информации о целях, правовых основаниях и способах обработки относящихся к ним данных.

Кроме того, рассматриваемая обязанность соответствует праву пользователя цифрового объекта на получение достоверной информации о его характеристиках и рисках (пп. 2) п. 2 ст. 39).

10. Пункт 6 статьи 24 определяет правовые основания, в соответствии с которыми собственники (владельцы) цифровых ресурсов должны/могут определять условия размещения, обработки и использования цифровых данных и цифровых записей на принадлежащих им цифровых ресурсах, а также доступом к ним.

К таким основаниям могут относиться не только положения законодательства, но договорные условия между собственником (владельцем) цифрового ресурса и пользователями, а также субъектами цифровых данных, чьи данные хранятся, обрабатываются и размещаются на цифровом ресурсе. При этом договорные условия не могут противоречить требованиям законодательства Республики Казахстан.

Статья 25. Объекты цифровой инфраструктуры

1. Объектом цифровой инфраструктуры признается совокупность материальных, технических и технологических средств, обеспечивающих размещение и среду функционирования цифровых объектов.

2. К объектам цифровой инфраструктуры относятся центры обработки данных, сети телекоммуникаций, средства связи и иные инфраструктурные объекты.

3. Требования к созданию, размещению, эксплуатации, модернизации, обеспечению устойчивости, целостности и кибербезопасности объектов цифровой инфраструктуры устанавливаются законодательством Республики Казахстан.

4. Объекты цифровой инфраструктуры могут находиться в государственной или частной собственности.

5. Государственные объекты цифровой инфраструктуры создаются в целях реализации государственных функций, оказания государственных услуг, защиты национальных интересов и обеспечения непрерывности государственного управления.

6. Негосударственные объекты цифровой инфраструктуры могут использоваться для обеспечения функционирования государственных цифровых объектов на основании законов Республики Казахстан.

Комментируемая статья определяет правовой режим объектов цифровой инфраструктуры как самостоятельной категории цифровых объектов, обеспечивающих создание среды для функционирования цифровой экономики.

Если цифровые данные, цифровые ресурсы, цифровые системы и цифровые платформы выступают объектами, в рамках которых непосредственно осуществляются обработка данных, оказание цифровых услуг и реализация цифровых процессов, то цифровая инфраструктура является материально-технологической основой их существования и функционирования. Например, портал eGov, банковское мобильное приложение или цифровая платформа электронной торговли не могут функционировать без центров обработки данных, сетей связи и иных инфраструктурных объектов, обеспечивающих их работу.

Кроме того, наличие устойчиво функционирующей инфраструктуры является необходимым условием реализации субъектами цифровой среды принадлежащих им прав.

Пункт 1 определяет объект цифровой инфраструктуры как совокупность материальных, технических и технологических средств, обеспечивающих размещение и среду функционирования цифровых

объектов. Законодатель исходит из функционального подхода, закрепленного пунктом 2 статьи 12 Цифрового кодекса, при котором определяющим признаком объекта цифровой инфраструктуры является его способность обеспечивать функционирование иных цифровых объектов. В отличие от цифровых ресурсов, цифровых систем и цифровых платформ, представляющих собой преимущественно нематериальные объекты, цифровая инфраструктура является материальной основой цифровых объектов.

1. Пункт 2 комментируемой статьи содержит открытый перечень объектов цифровой инфраструктуры. К ним отнесены центры обработки данных, сети телекоммуникаций, средства связи и иные инфраструктурные объекты. Законодатель использует формулировку «иные инфраструктурные объекты», руководствуясь принципом технологической нейтральности регулирования, что позволяет распространять действие статьи на новые виды инфраструктурных объектов.

Пункт 2 конкретизирует перечень объектов цифровой инфраструктуры, относя к ним центры обработки данных, сети телекоммуникаций, средства связи и иные инфраструктурные объекты.

Статьей 27 Цифрового кодекса предусмотрены специальные требования в отношении центров обработки данных.

Законом «О кибербезопасности» к объектам цифровой инфраструктуры отнесены: автоматизированные системы управления технологическими процессами.

2. Пункт 3 устанавливает, что требования к созданию, размещению, эксплуатации, модернизации, обеспечению устойчивости, целостности и кибербезопасности объектов цифровой инфраструктуры определяются законодательством Республики Казахстан.

Предметом регулирования Цифрового кодекса являются отношения, возникающие в цифровой среде при создании, обращении, хранении, передаче и использовании цифровых данных и цифровых объектов. Цифровой кодекс закладывает основы регулирования цифровых объектов именно в аспекте использования таких объектов для оборота данных (за исключением цифровых платформ, регулирование которых Цифровым кодексом выстроено как вокруг основной бизнес-модели цифровой экономики).

Пункт 3 носит отсылочный характер, поскольку объекты цифровой инфраструктуры различаются по своему назначению, техническому устройству и условиям эксплуатации. В связи с этим требования к их созданию, размещению, эксплуатации, модернизации, а также обеспечению их устойчивости, целостности и кибербезопасности устанавливаются не

только Цифровым кодексом, но и иными актами законодательства в сферах кибербезопасности, связи, строительства, электроэнергетики, национальной и информационной безопасности.

3. Пункт 4 предусматривает возможность нахождения объектов цифровой инфраструктуры как в государственной, так и в частной собственности.

Государственные и частные объекты цифровой инфраструктуры могут относиться к категории критически важных цифровых объектов (смотрите комментарий к статье 33 Цифрового кодекса).

Особенности правового регулирования объектов цифровой инфраструктуры как объектов гражданского оборота изложены в комментарии к статьям 1 и 20 Цифрового кодекса. Особенности правового регулирования государственных цифровых объектов установлены Разделом 5 Цифрового ккодекса.

4. Пункт 5 *«Государственные объекты цифровой инфраструктуры создаются в целях реализации государственных функций, оказания государственных услуг, защиты национальных интересов и обеспечения непрерывности государственного управления»* следует толковать в нескольких аспектах.

Прежде всего, комментируемый пункт определяет назначение государственных объектов цифровой инфраструктуры. Их создание обусловлено необходимостью реализации государственных функций, оказания государственных услуг, защиты национальных интересов и обеспечения непрерывности государственного управления. Таким образом, государственная цифровая инфраструктура может рассматриваться как один из элементов цифрового суверенитета государства.

Объекты цифровой инфраструктуры имеют важное значение не только для государства, но и для развития цифровой экономики. Центры обработки данных, сети связи и иные инфраструктурные объекты создают техническую основу для работы цифровых платформ, электронной коммерции, финансовых технологий и других цифровых сервисов.

Редакция пункта 5 статьи 25 позволяет сделать вывод об ограничениях вмешательства государства в конкурентную среду – законодатель императивно ограничивает цели создания государственных объектов цифровой инфраструктуры публичными задачами и не рассматривает государство в качестве участника цифрового рынка. Такой подход соответствует реализации принципа пропорционального и обоснованного участия государства в цифровой среде, закрепленного статьей 11 Цифрового кодекса.

В этой связи положения пункта 5 необходимо рассматривать также во взаимосвязи со статьей 8 Цифрового кодекса, закрепляющей принцип свободы создания, развития и применения цифровых технологий. Участие государства в создании объектов цифровой инфраструктуры не должно приводить к ограничению частной инициативы или созданию преимуществ для государственных субъектов на цифровых рынках. Напротив, государственная политика должна обеспечивать условия для развития конкуренции, привлечения частных инвестиций и расширения доступа бизнеса к инфраструктурным ресурсам.

Таким образом, пункт 5 отражает стремление законодателя обеспечить баланс между необходимостью государственного контроля над инфраструктурой, имеющей стратегическое значение для государства, и созданием условий для свободного развития технологий, цифрового предпринимательства и конкуренции в цифровой экономике.

5. Пункт 6 допускает использование негосударственных объектов цифровой инфраструктуры для обеспечения функционирования государственных цифровых объектов.

Это отражает современные форматы цифровой экономики, при которых государство может привлекать частные центры обработки данных, телекоммуникационные сети и иные инфраструктурные решения для размещения и эксплуатации государственных информационных ресурсов и систем. Вместе с тем использование частной инфраструктуры для государственных нужд допускается только на основании законов Республики Казахстан, что обусловлено необходимостью обеспечения контроля за использованием государственных данных, соблюдения требований информационной безопасности, а также защиты национальных интересов при эксплуатации государственных цифровых объектов на инфраструктуре, не принадлежащей государству.

Статья 28. Цифровые системы

1. Цифровой системой является функционально связанный комплекс цифровых ресурсов, использующий объекты цифровой инфраструктуры с целью обеспечения создания, сбора, обработки, хранения и распространения цифровых данных, а также автоматизирующий взаимодействие субъектов цифровой среды и (или) обеспечивающий оказание услуг в цифровой среде.

2. Владелец и (или) собственник цифровой системы вправе, если иное не установлено законами Республики Казахстан или владельцем и (или) собственником цифровых ресурсов, определять правила функционирования цифровой системы, включая условия перемещения и использования цифровых ресурсов, содержащихся в ней.

Владелец и (или) собственник цифровой системы обязаны обеспечивать надежность, целостность, защиту и кибербезопасность цифровой системы, а также соблюдать требования законодательства Республики Казахстан о персональных данных и их защите.

3. В случае, если владелец и (или) собственник цифровой системы не являются владельцами и (или) собственниками находящихся в ней цифровых ресурсов, порядок эксплуатации цифровой системы и доступа к цифровым ресурсам определяется соглашением между такими владельцами и (или) собственниками.

4. Создание, промышленная эксплуатация, сопровождение, развитие, интеграция, прекращение промышленной эксплуатации и защиты цифровых систем в защищенном исполнении, отнесенных к государственным секретам, осуществляются в соответствии с настоящим Кодексом, если иное не предусмотрено законодательством Республики Казахстан о государственных секретах.

1. Как указано в комментариях к статьям 1 и 20 Цифрового кодекса, законодатель при классификации и определении цифровых объектов руководствовался функциональным подходом. Статьей 12 Кодекса установлено, что правовое регулирование отношений в цифровой среде, осуществляется исходя из функциональных характеристик цифровых технологий и цифровых объектов (смотрите комментарий к пункту 2 статьи 12).

Основной функциональной характеристикой такого вида цифровых объектов как цифровые системы является: 1) организация функциональной связи между цифровыми ресурсами с целью обеспечения создания, обработки, хранения и распространения цифровых данных, а также 2) обеспечение автоматизации взаимодействия субъектов цифровой среды или 3) оказания услуг в цифровой среде.

Из указанного описания становится понятным наличие следующих функциональных особенностей, отличающих цифровые системы от иных видов объектов: 1) в состав цифровой системы входят иные цифровые объекты: цифровые ресурсы и цифровая инфраструктура; 2) посредством цифровых систем обеспечивается взаимодействие между субъектами цифровой среды, включая возможность оказания услуг (реализации товаров).

В Законе «Об информатизации» (теперь – Закон «О кибербезопасности»), отдельные положения которого утратили силу в связи с принятием Цифрового кодекса РК, понятие цифровой системы излагалось следующим образом: *«информационная система - организационно упорядоченная совокупность информационно-коммуникационных технологий, обслуживающего персонала и технической документации, реализующих определенные технологические действия посредством информационного взаимодействия и предназначенных для решения конкретных функциональных задач»* (пп. 12) п. 1).

Законом РК от 9 января 2026 года № 256-VIII «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам цифровизации, транспорта и предпринимательства», сопутствующем принятию Цифрового кодекса РК, понятие «информационная система» в действующем законодательстве Республики Казахстан изменено на «цифровая система».

Следует отметить, что на международном уровне определение цифровых (информационных) систем не является единым и общепризнанным. В современных международных актах используются разные варианты терминологии. Так, в Будапештской конвенции о киберпреступности используется понятие «компьютерная система - любое устройство или группа взаимосвязанных или смежных устройств, одно или более из которых, действуя в соответствии с программой, осуществляет автоматизированную обработку данных» (пп. а) ст. 1)³⁸.

В актах Европейского союза используются термины «сетевые и информационные системы» (NIS2) и «информационно-коммуникационные системы» (DORA), включающие в себя как сами устройства или их комплексы, так и данные.

Понятие «цифровая система» все шире используется в документах ОЭСР, ООН, Всемирного банка и иных международных организаций, однако, как правило, не имеет унифицированного определения.

³⁸ Конвенция о компьютерных преступлениях. ИС Параграф. [Электронный ресурс]. URL: https://prg.kz/document/?doc_id=30170556&pos=64;198 (дата обращения: 11.06.2026).

Исходя из изложенного, можно сделать вывод о том, что категория «цифровая (информационная) система» находится в процессе концептуального развития и не имеет устоявшегося понимания. **Определение цифровой системы, приведенное в настоящей статье, применимо исключительно для отношений в цифровой среде, регулируемых Цифровым кодексом и другими актами казахстанского законодательства в рамках казахстанской юрисдикции.**

В Цифровом кодексе нет указания на то, какие именно объекты могут быть отнесены к категории цифровых систем, что является реализацией в нормах Кодекса принципа технологической нейтральности правового регулирования – законодатель намерено не приводит перечня объектов, а перечисляет функциональные особенности с тем, чтобы при появлении новых цифровых объектов их можно было отнести к определенной категории, не изменяя положений Кодекса.

Ориентиром для практики применения и законотворческого процесса станет систематизация цифровых объектов в соответствии с видами цифровых объектов, предусмотренными Цифровым кодексом и иными законами Республики Казахстан, которая будет проведена Уполномоченным органом в сфере цифровизации.

Цифровым кодексом не предусмотрена обязанность для собственников (владельцев) цифровых объектов каким-либо образом присваивать принадлежащими им объектами вид и категорию. В соответствии с действующим порядком классификации объектов информатизации, установленным Приказом и.о. Министра по инвестициям и развитию Республики Казахстан от 28 января 2016 года № 135 собственники или владельцы негосударственных объектов информатизации проводят классификацию в соответствии с настоящими Правилами и на основании классификатора по собственной инициативе.

Определение вида цифрового объекта имеет практическое значение для установления его правового режима, объема прав и обязанностей собственника (владельца), особенностей оборота, требований кибербезопасности, а также применения специальных норм законодательства, регулирующих соответствующую категорию цифровых объектов.

Из существующих цифровых объектов к цифровым системам можно отнести цифровые платформы, мобильные приложения, ERP-системы, CRM-системы, портал госуслуг (eGov), налоговые системы, системы электронного документооборота и др.

2. Цифровая система, как следует из определения, является цифровым объектом с многоуровневой структурой, основой которой являются данные и цифровые записи, организованные в цифровых

ресурсах, совокупность которых представляет из себя цифровую систему. Каждый из элементов цифровой системы в свою очередь является самостоятельным объектом гражданского оборота и правового регулирования.

Такая многосоставность цифровых систем, а также особенности реализации вещных прав в отношении цифровых объектов может вызывать сложности в аспекте определения правового режима элементов цифровой системы.

Более того, отдельные элементы цифровой системы могут принадлежать разным собственникам (владельцам), что закреплено в пункте 3 комментируемой статьи.

Например, государственная информационная система может использовать данные из национальных регистров, программное обеспечение отдельного разработчика, облачную инфраструктуру специализированного провайдера, реализовывать государственные услуги посредством интерфейсов частных субъектов.

Таким образом, право собственности на цифровую систему не означает автоматического возникновения права собственности на каждый ее элемент. Объектом прав выступает сама система как функционально организованный комплекс, который соответствует признакам имущественного комплекса в аспекте гражданско-правового регулирования.

Как указано в комментарии к пункту 1 статьи 20 Цифрового кодекса: «Цифровая природа цифровых объектов, однако, должна обеспечивать (и не должна ограничивать) их оборотоспособность как объектов гражданских прав. В том числе, должна быть обеспечена возможность приобретения и осуществления права собственности на цифровые объекты, и возможность передачи прав на них от одного субъекта к другому в соответствии с законодательством Республики Казахстан (и это должно включать применение коллизионных норм и выбор применимого права в правоотношениях с участием иностранного элемента), если только оборот каких-то цифровых объектов или их видов не ограничивается законом».

Собственник системы вправе определять порядок функционирования самой системы, однако не может произвольно ограничивать права собственников цифровых ресурсов либо использовать принадлежащие им данные вне установленных законом или договором оснований.

Такому подходу соответствуют положения пунктов 2 и 3 комментируемой статьи, которыми закрепляются права собственников (владельцев) цифровых систем и входящих в них цифровых ресурсов самостоятельно определять правила функционирования цифровой системы,

включая условия перемещения и использования цифровых ресурсов, содержащихся в ней, а также совместно путем заключения соглашения определять порядок эксплуатации цифровой системы и доступа к содержащимся в ней цифровым ресурсам.

В силу того, что предмет регулирования Цифрового кодекса не позволяет включить весь комплекс правовых норм, необходимых для всестороннего определения правового режима разных видов цифровых объектов, детализация гражданско-правового регулирования цифровых систем будет реализована в процессе предстоящей модернизации Гражданского кодекса Республики Казахстан. Цифровой кодекс закладывает основы правового регулирования цифровых объектов как объектов гражданского оборота.

Особенности правового регулирования цифровых объектов как объектов гражданского оборота изложены в комментарии к статье 1 и статье 20 Цифрового кодекса.

3. Пункт 2 статьи 28 устанавливают обязанности собственников (владельцев) цифровых систем не только как объектов гражданского оборота, но и технологических объектов. К таким обязанностям относятся: обеспечение надежности, целостности, защиты и кибербезопасности цифровой системы, а также соблюдение требований законодательства Республики Казахстан о персональных данных и их защите.

Обязанности, установленные в пункте 2 комментируемой статьи, следует толковать во взаимосвязи с положениями статьи 38, которой установлены общие в отношении всех цифровых объектов права и обязанности их собственников (владельцев), а также с положениями статьи 24, которой определены обязанности собственников (владельцев) цифровых ресурсов, являющихся элементами цифровой системы. Кроме этого, собственники (владельцы) всех видов цифровых объектов, функционирование которых связано с оборотом, хранением, размещением цифровых данных, включая персональные должны соблюдать положения законодательства в сфере защиты персональных данных, а также международные требования к управлению данными.

Обязанности, перечисленные в пункте 2 статьи 28, направлены на поддержание безопасного, надежного и бесперебойного функционирования цифровой системы. Надежность цифровой системы представляет собой ее способность стабильно выполнять предусмотренные функции, сохранять работоспособность при сбоях и восстанавливаться после их устранения. Под целостностью цифровой системы понимается сохранение полноты, достоверности и неизменности содержащихся в ней данных, а также всех элементов системы и настроек.

Понятие «защита цифровых объектов» установлено статьей 53 Закона «О кибербезопасности»: «Защитой цифровых объектов является реализация комплекса правовых, организационных и технических мероприятий, направленных на сохранность цифровых объектов, предотвращение неправомерного и (или) непреднамеренного доступа и (или) воздействия на них». Законом также определены меры и требования к осуществлению защиты разных категорий цифровых объектов.

Все перечисленные обязанности должны исполняться собственниками (владельцами) цифровых систем на протяжении всего их жизненного цикла.

4. Пункт 4 статьи 28 устанавливает особенности правового режима цифровых систем в защищенном исполнении, данные и информация, размещенная в которых, относится к государственным секретам.

При этом статьей устанавливается приоритет Закона Пункт 4 статьи 28 устанавливает специальный режим для цифровых систем в защищенном исполнении с государственными секретами, приоритет законодательства о государственных секретах, которым определены повышенные требования к кибербезопасности для цифровых систем, содержащих специальные требования о передаче сведений в такие системы и обеспечении защиты таких сведений.

Статья 29. Цифровые платформы

1. Цифровая платформа - цифровой объект, обеспечивающий доступ к услугам в цифровой среде, данным, сервисам, товарам (работам, услугам), которые размещают субъекты цифровой среды, и позволяющий им взаимодействовать между собой.

2. Пользователи цифровых платформ в зависимости от деятельности на платформе делятся на пользователей цифровой платформы и бизнес-пользователя:

1) пользователи цифровой платформы - физические или юридические лица, использующие цифровую платформу для поиска, заказа или приобретения товаров, выполнения работ, оказания услуг, а также для иных потребительских или вспомогательных целей, не связанных с извлечением доходов, в том числе предпринимательской деятельностью;

2) бизнес-пользователь цифровой платформы - физическое или юридическое лицо, использующее цифровую платформу с целью продажи товаров, выполнения работ, оказания услуг или осуществления иной деятельности, связанной с извлечением дохода, в том числе предпринимательской деятельности.

3. Деятельность, осуществляемая на цифровой платформе, а также требования к пользователям цифровой платформы определяются отраслевым законодательством Республики Казахстан.

4. Требования к цифровым платформам устанавливаются в объеме, соразмерном выполняемым функциям, степени влияния на права неопределенного круга лиц и характеру контроля над цифровыми данными, услугами, товарами или результатами взаимодействия.

5. Владельцы цифровых платформ обязаны обеспечивать прозрачность условий использования, выраженных в пользовательском соглашении.

6. В случаях, когда бизнес-пользователь, владелец и (или) собственник цифровой платформы в соответствии с Налоговым кодексом Республики Казахстан исполняют обязанности налогового агента или налогоплательщика, такие обязанности осуществляются в порядке и объеме, которые установлены Налоговым кодексом Республики Казахстан.

1. Цифровые платформы – цифровые объекты, которые требуют особой определенности с точки зрения правового регулирования и четкого установления правового режима отношений, складывающихся в связи с их функционированием. Это обусловлено тем, что именно цифровые

платформы являются одной из ключевых экономических моделей, наряду с экосистемами, и формируют основу платформенной экономики.

К цифровым платформам в понимании статьи 29 относятся маркетплейсы, агрегаторы такси, магазины мобильных приложений, платформы бронирования услуг и иные цифровые сервисы, обеспечивающие взаимодействие различных групп пользователей

Широкое распространение цифровых платформ как бизнес-модели объясняется рядом факторов:

1. цифровые платформы обеспечивают возможность непосредственного взаимодействия в цифровой среде между многочисленными и разнородными группами пользователей;

2. платформенная модель снижает или устраняет традиционные барьеры взаимодействия между участниками рынка, обеспечивая доступ пользователей к сервисам, товарам и услугам, которые ранее были ограниченно доступны либо требовали значительных организационных и финансовых издержек;

3. цифровые платформы предоставляют поставщикам товаров и услуг готовую технологическую и организационную инфраструктуру для осуществления предпринимательской деятельности, что значительно снижает транзакционные издержки выхода на рынок. Для потребителей платформенная модель обеспечивает возможность выбора и сравнения товаров и услуг от разных поставщиков, а также упрощает процессы их поиска, сравнения и получения.

2. К моменту разработки и принятия Цифрового кодекса в законодательстве Республики Казахстан содержались определения отдельных видов цифровых платформ.

Так, пп. 2) п. 1 ст. 1 Закона «О цифровых активах в Республике Казахстан» определяет цифровую платформу по хранению и обмену обеспеченными цифровыми активами как *«совокупность информационно-коммуникационных технологий, построенных на основе распределенной платформы данных, реализующих определенные информационные взаимодействия и предназначенных для решения конкретных функциональных задач, предоставляющих возможность информационного обмена»*.

В Законе «Об онлайн-платформах и онлайн-рекламе» (пп. 10) ст. 1) онлайн-платформа определена как интернет-ресурс или программное обеспечение, функционирующее в сети Интернет, предназначенное для получения, производства или размещения, распространения, хранения контента на онлайн-платформе пользователем онлайн-платформы посредством созданного им аккаунта, публичного сообщества, за

исключением интернет-ресурса или программного обеспечения, функционирующего в сети Интернет, предназначенного для предоставления финансовых услуг и электронной коммерции.

Необходимость внесения соответствующих корректировок в Закон «Об онлайн-платформах и онлайн-рекламе» в связи с принятием Цифрового кодекса подробно анализировалось автором в статье «Соотношение правовых режимов цифровых платформ и онлайн-платформ в свете принятия Цифрового кодекса Республики Казахстан»³⁹.

Закон «О регулировании торговой деятельности» содержит определения нескольких видов цифровых платформ. Так, цифровые платформы, предназначенные для осуществления электронной торговли (маркетплейсы), определяются как электронная торговая площадка – интернет-ресурс, обеспечивающий инфраструктуру участникам электронной торговли, в том числе заключение договоров между ними на оказание работ и услуг с использованием информационно-коммуникационных технологий (пп. 58) ст. 1). Цифровые платформы-классифайды определяются как информационно-рекламные торговые площадки – интернет-ресурсы, содержащие рекламные (информационные) сведения о продавцах, а также о товарах, работах и услугах с целью организации их купли-продажи. (пп. 2) ст. 1).

Одна из целей включения в Цифровой кодекс, как акт высшей юридической силы в сфере отношений в цифровой среде, определения «цифровая платформа» заключалась в следующем: обеспечить единое понимание и применение этого понятия в других нормативных актах, регулирующих отдельные отношения, связанные с функционированием платформ, без изменения или искажения его содержания. Автор настоящего комментария также является автором положений, определяющих правовой режим цифровых платформ.

3. *«Цифровая платформа – цифровой объект, обеспечивающий доступ к услугам в цифровой среде, данным, сервисам, товарам (работам, услугам), которые размещают субъекты цифровой среды, и позволяющий им взаимодействовать между собой»* – такое технологически нейтральное определение цифровой платформы, содержащееся в п. 1 ст. 29 Цифрового кодекса, является родовым по отношению к отдельным видам цифровых платформ: социальным сетям, маркетплейсам, классифайдам, агрегаторам, магазинам приложений и пр.

В контексте правотворческой деятельности и дальнейшего формирования правового регулирования цифровых платформ

³⁹ Бычкова Е.С. Соотношение правовых режимов цифровых платформ и онлайн-платформ в свете принятия Цифрового кодекса Республики Казахстан – PRG.kz [Электронный ресурс]. URL: https://prg.kz/document/?doc_id=35647225 (дата обращения: 11.06.2026).

принципиальное значение имеет закрепление **правового режима объекта**. В структуре Цифрового кодекса такой подход воспринимается как логичный и системный, однако в правоприменительной и нормотворческой практике нередко наблюдается отождествление платформ с субъектами права, что приводит к попыткам наделения их самостоятельными обязанностями и ответственностью.

Закрепление правового режима цифровых платформ как объектов регулирования предполагает необходимость более глубокого и дифференцированного подхода к определению объема прав и обязанностей и распределению ответственности между субъектами, вовлеченными в функционирование платформы, включая собственников, владельцев, операторов, пользователей.

В отличие от других видов цифровых объектов, правовой режим которых определяется в двух аспектах – как объектов гражданско-правовых отношений и технологических объектов.

Цифровые платформы определены Цифровым кодексом как бизнес-модель, характерная для новой цифровой экономики. Технологически платформы представляют из себя цифровые системы.

Определение цифровой платформы, содержащееся в приведенном п. 1 ст. 29, отражает ее ключевую основную функциональную характеристику как бизнес-модели – **обеспечение взаимодействия разных многочисленных и даже неограниченных групп пользователей**. «Платформа как бизнес-модель представляет собой модель обеспечения посредством технологической площадки прямого взаимодействия и осуществления трансакций между субъектами с использованием новых способов и форм взаимодействия, создания ценности и ценообразования. Это отличает платформы от торговцев и классических посредников, где отсутствует прямое взаимодействие заинтересованных друг в друге сторон, а также от вертикально интегрированных компаний, которые объединяют одну сторону рынка в рамках единой структуры собственности»⁴⁰.

Тем самым в Кодексе фактически закрепляется **посредническая природа цифровых платформ**. При этом, следует отметить, что понятие «информационный посредник» в нормах Цифрового кодекса прямо не используется.

В 2013 году в Гражданский кодекс Российской Федерации были внесены положения, определяющие разграничение ответственности и

⁴⁰ Гелисханов И.З., Юдина Т.Н., Бабкин А.В. Цифровые платформы в экономике: сущность, модели, тенденции развития. Научно-технические ведомости СПбГПУ. Экономические науки. 2018. Т. 11, № 6. С. 22–36. DOI: 10.18721/JE.11602. [Электронный ресурс]. URL: <https://cyberleninka.ru/article/n/tsifrovyye-platforny-v-ekonomike-suschnost-modeli-tendentsii-razvitiya> (дата обращения: 11.06.2026).

требования по соблюдению прав интеллектуальной собственности между «информационными посредниками» и пользователями, размещающими контент или информацию. Нужно отметить, что ГК РФ (ст. 1253.1) определяет информационного посредника как субъекта отношений – лицо, которым может являться владелец платформы или хостинг-провайдер. Пунктом 77 Постановления Пленума Верховного суда РФ (разъяснительный акт, принимаемый в целях формирования единообразной практики нижестоящими судами) определено, что суд в каждом конкретном случае устанавливает в зависимости от вида осуществляемой деятельности, является ли конкретное лицо информационным посредником или нет⁴¹.

Отдельные казахстанские юристы экстраполируют статус информационных посредников (в устных рассуждениях и видео на своих страницах в социальных сетях по вопросам разграничения ответственности между площадками и пользователями) на казахстанские площадки, однако, отдельные выводы должны быть откорректированы с учетом принятия Цифрового кодекса и отсутствия в казахстанском законодательстве понятия и регламентации деятельности «информационных посредников».

4. Закрепление на уровне Цифрового кодекса базового понятия цифровой платформы и общих принципов регулирования формирует единую понятийную и концептуальную регуляторную основу, применимую ко всем видам платформ независимо от специфики реализуемых на них сервисов.

В развитие данного подхода сформулирован пункт 3 статьи 29, предусматривающий применение соответствующего отраслевого законодательства к деятельности, осуществляемой на цифровой платформе, а также требований к ее пользователям. Указанная норма определяет не только структуру регулирования и правоприменения, но и вектор дальнейшего развития законотворческой практики в сфере регулирования платформенных рынков – через дополнение и уточнение отраслевых актов, а не посредством разработки комплексных актов в отношении каждого вида платформ или платформенной экономики в целом.

По мнению автора настоящего комментария, такой подход способствует более точному и обоснованному распределению прав и обязанностей между участниками платформенных отношений, поскольку позволяет регулировать не абстрактную «платформу», а конкретные отношения между субъектами определенной экономической деятельности.

Цифровой кодекс не содержит классификация видов платформ и не предусматривает отсылки к иному акту, устанавливающему такую

⁴¹ Постановление Пленума Верховного суда Российской Федерации от 23 апреля 2019 года № 10 «О применении части четвертой Гражданского кодекса Российской Федерации». [Электронный ресурс]. URL: <https://base.garant.ru/72230696/> (дата обращения: 18.03.2026).

классификацию. По мнению автора, законодательное закрепление жесткой классификации платформ нецелесообразно, поскольку одна и та же платформа может одновременно выполнять несколько функций и подпадать под действие различных отраслевых правовых режимов. Кроме того, попытка зафиксировать в законодательных нормах набор признаков, характерных для одного вида платформ, приведут к ограничению развития платформенной экономики, поскольку технологии позволяют сочетать и предлагать уникальные новые сервисы.

В казахстанском законодательстве есть пример акта, разработанного в целях регулирования конкретного вида платформ – онлайн-платформ, предметом которого фактически является размещение контента пользователями социальных сетей. Такой регуляторный подход не соответствует положениям Цифрового кодекса, о чем автор комментария подробно рассуждал в своей публикации «Соотношение правовых режимов цифровых платформ и онлайн-платформ в свете принятия Цифрового кодекса Республики Казахстан»⁴².

Кроме того, отказ от законодательного закрепления исчерпывающей классификации цифровых платформ соответствует принципу технологической нейтральности, закрепленному статьей 12 Цифрового кодекса. Правовое регулирование должно учитывать выполняемые платформой функции и характер возникающих отношений в связи с использованием платформой.

5. Как было указано, технологически платформы относятся к такому виду цифровых объектов как цифровые системы, технологической особенностью которой является возможность обеспечения взаимодействия значительных по количеству групп пользователей. Особенности правового регулирования цифровых систем как объектов гражданского оборота детально изложены в комментарии к статьям 1, 20, 24, 25.

6. Как экономическая модель и действующий бизнес платформа представляет из себя многосоставную систему объектов, процессов и отношений: программное обеспечение, интерфейс, базы данных, домены, инфраструктурная составляющая (цод, фулфилмент, склады и пр.); заключение сделок, обеспечение платежей, интеграция с базами данных, договорные отношения с бизнес-пользователями, реализация основного оффлайн сервиса (доставка, перевозка, предоставление транспорта в аренду и пр.), используемые для достижения единого результата.

Исходя из изложенного, цифровая платформа в аспекте ее определения как объекта гражданско-правовых отношений приобретает **черты**

⁴² Бычкова Е.С. Соотношение правовых режимов цифровых платформ и онлайн-платформ в свете принятия Цифрового кодекса Республики Казахстан. PRG.kz. 2026 [Электронный ресурс]. URL: https://prg.kz/document/?doc_id=35647225 (дата обращения: 11.06.2026).

имущественного комплекса, определенные статьей 119 Гражданского кодекса (Общая часть): «п 2. В состав предприятия как имущественного комплекса входят все виды имущества, предназначенные для его деятельности, включая здания, сооружения, оборудование, инвентарь, сырье, продукцию, право на земельный участок, права требования, долги, а также права на обозначения, индивидуализирующие его деятельность (фирменное наименование, товарные знаки), и другие исключительные права, если иное не предусмотрено договором».

3. В научной литературе также высказывается мнение о том, что цифровые платформы являются сложными объектами и имущественным комплексом: «Очевидно, что цифровая платформа не может быть признана простым объектом гражданских правоотношений. Она состоит из различных структурных элементов (база данных, интернет-сайт, компьютерные программы, используемые для обработки информации и обеспечивающие взаимодействие с пользователями, а также в целом функционирование платформы), каждый из которых может быть отнесен к различным объектам гражданских прав. При этом все указанные объекты используются по единому назначению. Соответственно, цифровая платформа в гражданском обороте может рассматриваться в качестве сложного объекта. Признание цифровой платформы единым сложным объектом интеллектуальных прав дает основание для объединения всех ее составляющих. Однако цифровые платформы, используемые в предпринимательской деятельности, как правило, индивидуализированы в обороте, в силу чего средства индивидуализации могут стать их частью. Помимо этого, платформы, определяемые через понятие информационных систем, в том числе интегрирующие, например облачные сервисы, могут в качестве структурного элемента включать технические средства, позволяющие функционировать информационной системе в целом. В последнем случае цифровая платформа может приобрести черты имущественного комплекса, содержащего в себе различные виды имущества, в частности вещи, имущественные (в том числе исключительные) права».⁴³

«Платформа представляет собой сложный объект, в который объединены в функциональное единство отдельные элементы (программы для ЭВМ, базы данных, произведения, а также оборудование и пр.). Определение платформы как сложного объекта необходимо для объяснения единства правовой судьбы отдельных элементов платформы. В силу разнородности объектов, образующих сложный объект, можно говорить, с одной стороны, о праве на каждый из объектов, входящих в данный

⁴³ Аюшеева И. З. Правовой режим цифровых платформ как объектов гражданских прав. Lex russica. 2025. Т. 78. № 11. С. 44–53. [Электронный ресурс]. URL: <https://lexrussica.msal.ru/jour/article/view/4812/1703> (дата обращения: 11.06.2026).

комплекс, и это право зависит от вида объекта и правоспособности обладателя, и, с другой стороны, о праве на платформу как единый комплекс, - в последнем случае следует говорить о принадлежности этого комплекса лицу на вещном праве, соответствующем правоспособности»⁴⁴.

Такой подход согласуется с общей позицией, изложенной в комментариях к статьям 1 и 20 Цифрового кодекса, согласно которой цифровые объекты должны обладать оборотоспособностью и участвовать в гражданском обороте наравне с иными объектами гражданских прав, если ограничения их оборота прямо не установлены законом.

6. Пункт 2 статьи 29 определяет ключевой подход к регулированию цифровых платформ как бизнес-модели новой цифровой экономики, заключающийся в дифференциации категорий пользователей платформ и их прав и обязанностей. Как было указано, особенностью цифровых платформ как цифровых объектов является обеспечение взаимодействия между разнородными неограниченными группами пользователей.

Пункт 2 определяет категории пользователей цифровых платформ в зависимости от того, какую деятельность они осуществляют посредством платформы: бизнес-пользователи, осуществляющие предпринимательскую деятельность, и пользователей, чье пользование платформой не связано с извлечением дохода.

Такой подход уже можно назвать общепринятым. Так, в Digital Services Act – одном из основных актов Европейского Союза, регулирующем деятельность цифровых платформ, определены специальные положения в отношении бизнес-пользователей (business users) и потребителей (consumers) – любых физических лиц, которые действуют в целях, выходящих за рамки их торговой, коммерческой, ремесленной или профессиональной деятельности (перевод автора) (п (с) статьи 3 главы I)⁴⁵.

Определение бизнес-пользователя – как любого частного лица, действующего в коммерческом или профессиональном качестве, или любого юридического лица, действующего посредством онлайн посреднического сервиса и предлагающего товары или услуги потребителям в рамках его торговой, предпринимательской или ремесленнической деятельности» (перевод автора) закреплено в Регламенте (ЕС) 2019/1150 Европейского парламента и Совета от 20 июня 2019 г. о

⁴⁴ Филиппова С. Ю., Харитонов Ю. С. Цифровые платформы в праве и право цифровых платформ: новые вызовы законодателью и пути их решения. Правоведение. 2025. Т. 69, № 1. С. 58–75. DOI: 10.21638/spbu25.2025.104 [Электронный ресурс]. URL: <https://doi.org/10.21638/spbu25.2025.104> (дата обращения: 11.06.2026).

⁴⁵ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). An official website of the European Union. [Электронный ресурс]. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065> (дата обращения: 11.06.2026).

содействии справедливости и прозрачности для бизнес-пользователей онлайн-посреднических услуг (Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services) (п. (1) ст. 2)⁴⁶.

Федеральный закон от 31.07.2025 N 289-ФЗ «Об отдельных вопросах регулирования платформенной экономики в Российской Федерации» также закрепляет две основные категории пользователей цифровых посреднических платформ: партнеров (лиц, реализующих товары или оказывающих услуги) и пользователей (пп. 4,7 ст. 2)⁴⁷.

Основная цель закрепления категорий пользователей в Цифровой кодекс заключается в институционализации различий между субъектами платформенных отношений: бизнес-пользователями как субъектов предпринимательской деятельности, а пользователей, выступающих в качестве экономически и информационно более уязвимой стороны. При этом пользователи платформ – физические лица подпадают под действие законодательства о защите прав потребителей, которым предусмотрены специальные гарантии и механизмы защиты их прав.

Напротив, бизнес-пользователи рассматриваются как участники, способные нести повышенный объем рисков и ответственности, а также соблюдать требования применимого законодательства.

7. Пунктом 4 статьи 29 закреплён принцип соразмерности регулирования: *«Требования к цифровым платформам устанавливаются в объеме, соразмерном выполняемым функциям, степени влияния на права неопределенного круга лиц и характеру контроля над цифровыми данными, услугами, товарами или результатами взаимодействия»*.

Данный подход можно квалифицировать как risk-based regulation, который, однако, должен быть реализован с учетом особенностей развития технологий и в соответствии с ключевым принципом о свободе создания, развития и применения цифровых технологий, установленным статьей 8 Цифрового кодекса.

Такой подход соответствует принципу пропорционального и обоснованного участия государства в цифровой среде, закреплённому статьей 11 Цифрового кодекса. Регуляторное воздействие должно определяться не самим фактом существования цифровой платформы, а

⁴⁶ Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services. [Электронный ресурс]. URL: <https://eur-lex.europa.eu/eli/reg/2019/1150/oj/eng> (дата обращения: 11.06.2026).

⁴⁷ Федеральный закон от 31.07.2025 N 289-ФЗ «Об отдельных вопросах регулирования платформенной экономики в Российской Федерации». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_511088/ (дата обращения: 11.06.2026).

степенью влияния ее деятельности на права пользователей, конкуренцию, оборот цифровых данных и публичные интересы.

Пункт 4 имеет ключевое значение для развития законодательства в отношении цифровых платформ – с одной стороны, он ограничивает универсальный подход к установлению требований, исключая автоматическое возложение на их собственников (владельцев) обязанностей за все аспекты деятельности, осуществляемой посредством платформ.

С другой стороны, норма направлена на предотвращение попыток возложить на собственников (владельцев) платформ дополнительные функции, которые по своей природе не могут или не должны осуществляться частными субъектами (разрешение споров в сфере интеллектуальной собственности, проверка соответствия субъектов разрешениям и лицензиями, ведение реестров и пр.).

Подход, определенный пунктом 4, должен соблюдаться и в правоприменительной практике при рассмотрении спорных ситуаций. Так, при определении субъекта ответственности, необходимо анализировать не только применимое законодательство, но и конкретные договорные конструкции. Даже в рамках одной категории платформы могут выполнять как преимущественно посредническую функцию, так и иметь глубоко интегрированные в процесс оказания услуг сервисы.

Автор настоящего комментария подробно рассуждал об особенностях отдельных бизнес-моделей маркетплейсов и применимой ответственности за контрафактную продукцию в своей статье «Решат ли маркетплейсы проблему оборота контрафакта и товаров низкого качества в Казахстане»⁴⁸.

8. Пункт 5 статьи 29 устанавливает обязанность владельцев цифровых платформ обеспечивать прозрачность условий использования платформы, закрепленных в пользовательском соглашении.

Пользовательские отношения являются основным инструментом структурирования отношений между участниками платформенного рынка, а также юридической основой для определения объема и пределов ответственности собственника (владельца) платформы.

При этом требование прозрачности означает недопустимость произвольного или скрытого закрепления условий, ограничивающих ответственность владельца платформы.

Обязанность по обеспечению прозрачности условий использования цифровой платформы направлена на реализацию принципа свободного и

⁴⁸ Бычкова Е.С. Решат ли маркетплейсы проблему оборота контрафакта и товаров низкого качества в Казахстане. [Электронный ресурс]. URL: <https://www.zakon.kz/mnenie/6460500-reshat-li-marketpleysy-problemu-oborota-kontrafakta-i-tovarov-nizkogo-kachestva-v-kazakhstane.html> (дата обращения: 11.06.2026).

осознанного волеизъявления человека в цифровой среде, закрепленного пунктом 2 статьи 5 Цифрового кодекса. Пользователь должен иметь возможность понимать последствия присоединения к условиям платформы, объем своих прав и обязанностей, а также правила обработки относящихся к нему данных.

В платформенных отношениях условия пользования определяются собственником (владельцем) платформы в одностороннем порядке и принимаются пользователем путем присоединения. В связи с этим требования прозрачности фактически являются способом обеспечения баланса интересов участников цифровой среды и предупреждения злоупотребления экономическими или технологическими преимуществами собственников (владельцев) платформы.

Вместе с тем, ни в Цифровом кодексе, ни в иных нормативных правовых актах Республики Казахстан понятие пользовательского соглашения не закреплено. Аналогично в научной доктрине подход к определению гражданско-правовой природы пользовательских соглашений как договора остается дискуссионным:

«Применяемые по аналогии закона гражданско-правовые нормы, регулирующие схожие по правовой природе и признакам гражданско-правовые отношения по оказанию услуг, выступают важным регулятором пользовательских соглашений, которые по своей сути можно рассматривать и анализировать как смешанные договоры, положения которых содержат нормы (элементы правовой конструкции) различных гражданско-правовых договоров, урегулированных ГК РФ, например, договора возмездного оказания услуг, лицензионного договора, агентского договора. Такие соглашения по своей природе представляют собой юридически значимый договор, заключаемый способом публичной оферты. Согласно п. 2 ст. 437 ГК РФ, публичной офертой признается содержащее все существенные условия договора предложение, из которого усматривается воля лица, делающего предложение, заключить договор на указанных в предложении условиях с любым, кто отзовется⁴⁹.

«На основании приведенных определений можно выделить следующие признаки пользовательских соглашений: 1) выступает в качестве правил использования ПО; 2) может рассматриваться в качестве публичной оферты; 3) согласие с его условиями выступает обязательным для любого пользователя. Таким образом, пользовательское соглашение представляет собой публичный договор, заключаемый с любым

⁴⁹ Гасанов А. Я. Правовая природа пользовательских соглашений оказания услуг с использованием цифровых технологий. Вестник Московского университета МВД России. 2022. № 1. С. 86–90. [Электронный ресурс]. URL: <https://cyberleninka.ru/article/n/pravovaya-priroda-polzovatelских-soglasheniy-okazaniya-uslug-s-ispolzovaniem-tsifrovyyh-tehnologiy/viewer> (дата обращения: 11.06.2026).

пользователем ПО, который направлен на урегулирование прав и обязанностей правообладателя и пользователя (подписчика)⁵⁰.

На момент принятия Цифрового кодекса особые требования к пользовательскому соглашению онлайн-платформ определены Законом «Об онлайн-платформах и онлайн-рекламе»: обязанность собственника онлайн-платформы создает возможность ознакомления с пользовательским соглашением, в том числе, кратким изложением его основных условий на казахском языке (п. 1 ст. 5.); обязанность описать в пользовательском соглашении параметры, используемые в рекомендательной системе (п. 1 ст. 12).

Пользовательские соглашения транзакционных платформ, пользователи которых могут быть квалифицированы как потребители в соответствии Законом «О защите прав потребителей», должны соответствовать положениям указанного Закона.

9. Общественные отношения, возникающие в связи с функционированием цифровых платформ, регулируются различными отраслями права: гражданским, налоговым, трудовым, антимонопольным, о кибербезопасности и пр. Цифровой кодекс не является комплексным актом, регулирующим указанные отношения.

Пункт 6 статьи 29 является отсылочным и мог бы быть продолжен указанием на применение Предпринимательского кодекса, Социального кодекса и пр.

⁵⁰ Гаврилов В.Н., Чиркаев С.А., Рассказов А.А. Правовая природа пользовательского соглашения в России. Вестник Саратовской государственной юридической академии. 2023. № 3 (152). С. 155–161. [Электронный ресурс]. URL: <https://cyberleninka.ru/article/n/pravovoe-regulirovanie-polzovatelskogo-soglasheniya-v-rossii> (дата обращения: 11.06.2026).

Глава 5. ПРОДУКТЫ ЦИФРОВЫХ ДАННЫХ И ИХ ОБОРОТ

Статья 30. Продукт цифровых данных

1. Продукт цифровых данных – агрегированный, формализованный результат обработки цифровых данных, включающий структурированные или иным образом преобразованные цифровые данные, пригодные для использования, обмена и (или) оборота в цифровой среде.

2. Структура, качество и метаданные продуктов цифровых данных государственных органов, государственных юридических лиц и субъектов квазигосударственного сектора регулируются в соответствии с требованиями по управлению данными.

3. Продукт цифровых данных на платформе обмена и оборота продуктов цифровых данных может быть предметом сделок, отчуждения и передачи на условиях, определенных владельцем, за исключением общедоступной информации, предусмотренной законодательством Республики Казахстан.

4. Продукт цифровых данных на платформе обмена и оборота продуктов цифровых данных должен обладать следующими свойствами:

1) не должен содержать персональные данные, допускающие возможность идентификации субъектов персональных данных прямым и (или) косвенным методами;

2) создан, обработан и структурирован в соответствии с требованиями к безопасности и качеству цифровых данных;

3) включает необходимые метаданные о составе, структуре, назначении и условиях использования.

Статья 31. Платформы обмена и оборота продуктов цифровых данных

1. Платформа обмена и оборота продуктов цифровых данных – цифровая платформа, обеспечивающая доступ к размещенным на ней продуктам цифровых данных с установленными условиями их обмена и оборота в соответствии с настоящим Кодексом и законодательством Республики Казахстан.

2. Государственные органы, государственные юридические лица, субъекты квазигосударственного сектора и субъекты частного предпринимательства, осуществляющие деятельность на территории Республики Казахстан, вправе создавать платформы обмена и оборота продуктов цифровых данных с соблюдением единых требований в сферах

цифровизации и обеспечения кибербезопасности, а также правил функционирования платформ обмена и оборота продуктов цифровых данных, утвержденных уполномоченным органом по развитию экономики данных по согласованию с уполномоченным органом.

3. Уполномоченный орган по развитию экономики данных – государственный орган, осуществляющий руководство в сферах стратегического планирования, проведения реформ и в области государственной статистики.

4. Платформы обмена и оборота продуктов цифровых данных подлежат включению в реестр платформ обмена и оборота продуктов цифровых данных при соответствии критериям и в порядке, которые определены уполномоченным органом по развитию экономики данных. 5. Собственники и (или) владельцы платформ обмена и оборота продуктов цифровых данных обязаны:

1) обеспечивать создание и ведение перечня продуктов цифровых данных;

2) обеспечивать условия доступа, обмена и использования продуктов цифровых данных;

3) предотвращать несанкционированный доступ, утечку и трансграничную передачу продуктов цифровых данных, если такая передача ограничена законами Республики Казахстан.

6. Уполномоченный орган по развитию экономики данных осуществляет мониторинг платформ обмена и оборота продуктов цифровых данных.

7. С момента начала деятельности собственник и (или) владелец платформ обмена и оборота продуктов цифровых данных обязаны направить уведомление о начале или прекращении деятельности или действий в уполномоченный орган по развитию экономики данных в соответствии с законодательством Республики Казахстан о разрешениях и уведомлениях.

8. Уполномоченный орган по развитию экономики данных разрабатывает и утверждает типовую методику оценки стоимости продуктов цифровых данных для государственных органов, государственных юридических лиц и субъектов квазигосударственного сектора по согласованию с уполномоченным органом.

9. Собственникам и (или) владельцам платформ обмена и оборота продуктов цифровых данных запрещается:

1) осуществлять оборот исходных (необработанных) данных, включая персональные данные, если иное не установлено законами Республики Казахстан;

2) осуществлять размещение или хранение продуктов цифровых данных вне территории Республики Казахстан, если такое размещение или хранение ограничено;

3) передавать продукты цифровых данных третьим лицам без согласия собственника и (или) владельца продукта цифровых данных, за исключением случаев, предусмотренных законодательством Республики Казахстан.

ОБЩИЙ КОММЕНТАРИЙ К СТАТЬЯМ 30 и 31

1. Глава 5 Цифрового кодекса, включающая две статьи 30 и 31, закрепляет концептуальные основы правового регулирования экономики данных в Республике Казахстан.

В отличие от большинства положений Кодекса, направленных на регулирование отдельных видов цифровых объектов или отношений, положения данной главы определяют подходы к вовлечению данных и продуктов их обработки в экономический оборот.

Указанные статьи регламентируют единый комплекс отношений, в связи с чем комментарий к данным статьям изложен как анализ общей концепции организации рынка оборота продуктов цифровых данных на платформах обмена и оборота продуктов цифровых данных, а не как последовательный комментарий к каждому пункту.

Для понимания значения рассматриваемых статей необходимо определить их место в системе Цифрового кодекса. Законодатель выделил положения, регламентирующие основы функционирования рынка продуктов цифровых данных в отдельную главу, которая может получить дальнейшее развитие по мере формирования правового регулирования экономики данных. Так, если Главы 3 и 4 Раздела 2 Кодекса определяют правовой режим объектов цифровой среды как объектов гражданского оборота и технологических объектов, то **Главу 5 можно истолковать как закрепление правовых основ нового сегмента цифровой экономики – рынка продуктов цифровых данных.**

На концептуальный характер Главы 5 указывает также упоминание в статье 31 уполномоченного органа в сфере развития экономики данных, осуществляющего руководство в сферах стратегического планирования, проведения реформ и в области государственной статистики. Это

свидетельствует о переходе на уровне государства от технологических процессов цифровизации к развитию и регламентации новых форматов экономической деятельности.

2. Ключевыми элементами функционирования рынка продуктов цифровых данных, предусмотренного статьями 30 и 31 Цифрового кодекса, являются продукты цифровых данных и платформы обмена и оборота продуктов цифровых данных. Поэтому для понимания содержания комментируемых статей целесообразно рассмотреть особенности их правовой и экономической природы.

В отличие от цифровых данных, которые являются исходным ресурсом цифровой экономики, продукт цифровых данных представляет собой результат их агрегирования, структурирования или иного преобразования, а также обладает самостоятельной практической и экономической ценностью. Экономическая ценность продукта цифровых данных определяется не только содержащимися в нем данными данных, но и информацией об их происхождении, структуре, качестве, и условиях использования, выраженной в метаданных.

В этой связи продукт цифровых данных следует рассматривать не особый вид цифровых данных, а как самостоятельный объект цифровой среды, являющийся результатом «переработки» цифровых данных. В определенной степени его можно сопоставить с соотношением нефти как исходного ресурса и различных нефтепродуктов как результатов переработки, которые в результате имеют самостоятельную экономическую ценность. Аналогичным образом продукты цифровых данных формируются на основе цифровых данных, но приобретают новые свойства и самостоятельную ценность и значение.

Следует отметить, что понятие «продукт цифровых данных» на момент подготовки настоящего Комментария законодательно закреплено только в Республике Казахстан и не имеет общепризнанного определения в международных документах. Вместе с тем понятие «data product» широко используется в профессиональной литературе и документах по управлению данными таких компаний как IBM, Microsoft, Google, занимающихся вопросами управления данными и развития экономики данных.

Отсутствие унифицированного подхода к определению продуктов цифровых данных на уровне международных актов может усложнить квалификацию трансграничных сделок и выбор применимого правового режима.

Платформа обмена и оборота продуктов цифровых данных представляет интерес, не как особый объект цифровой среды, а как механизм организации рынка продуктов цифровых данных. Ее функциональное назначение заключается в создании условий для поиска,

предоставления, обмена, использования и оборота продуктов цифровых данных между субъектами цифровой среды.

Такой вывод подтверждается Правилами функционирования платформ обмена и оборота продуктов цифровых данных, утвержденных Приказом Председателя Агентства по стратегическому планированию и реформам РК от 30 апреля 2026 года № 5 (далее по тексту комментируемой статьи – «Правила функционирования платформ»). В отличие от обычных электронных торговых площадок, платформы обмена и оборота продуктов цифровых данных обеспечивают идентификацию участников, ведение перечней продуктов цифровых данных, проверку соблюдения обязательных требований, фиксацию операций, обеспечение прослеживаемости оборота и соблюдение требований безопасности. **Тем самым платформа выполняет не только посредническую, но и организационную функцию, обеспечивая формирование и функционирование рынка продуктов цифровых данных.**

Платформы оборота и обмена продуктов цифровых данных не указаны в качестве самостоятельного вида цифровых объектов в статье 20 Цифрового кодекса. Они относятся к такому виду цифровых объектов как цифровые платформы (которые в свою очередь как технологические объекты являются цифровыми системами), обеспечивающие взаимодействие субъектов цифровой среды по поводу особого вида цифровых объектов – продуктов цифровых данных.

Пункт 2 статьи 31 устанавливает, что создавать платформы обмена и оборота цифровых данных могут не только субъекты частного предпринимательства, но также государственные органы, государственные юридические лица и субъекты государственного сектора. Таким образом, государство не ограничивается ролью регулятора рынка продуктов цифровых данных, но становится его участником.

Данное положение должно быть реализовано в соответствии с учетом принципа пропорционального и обоснованного участия государства в цифровой среде, установленного статьей 11 Цифрового кодекса. Соответственно, государственное участие в создании и эксплуатации платформ обмена и оборота продуктов цифровых данных допускается исключительно в целях реализации государственных функций, оказания государственных услуг, обеспечения безопасности, устойчивости и доступности цифровой инфраструктуры при соблюдении требований недопущения необоснованного вмешательства в конкурентную среду.

3. Цифровым кодексом платформы обмена и оборота продуктов цифровых данных не определены в качестве исключительных площадок для осуществления гражданско-правовых сделок с таким видом объектов цифровой среды как продукты цифровых данных.

Кроме того, Типовой методикой оценки стоимости продуктов цифровых данных для государственных органов, государственных юридических лиц и субъектов квазигосударственного сектора, утвержденной Приказом Председателя Агентства по стратегическому планированию и реформам Республики Казахстан от 27 апреля 2026 года № 3 (далее по тексту комментируемой статьи – «Типовая методика») определены случаи оценки стоимости продуктов цифровых данных, не связанных с оборотом продуктов цифровых данных на платформах: при определении стоимости предмета залога; при определении стоимости имущественных вкладов в уставный капитал; при определении стоимости имущества должника в ходе процедур банкротства; при определении стоимости безвозмездно полученного имущества и пр.

Исходя из изложенного можно сделать вывод о том, что оборот продуктов цифровых данных возможен и вне платформ обмена и оборота продуктов цифровых данных. При этом, законодательством Республики Казахстан не устанавливается специальных требований к продуктам цифровых данных, оборот которых происходит за пределами платформ, за исключением продуктов цифровых данных государственных органов, государственных юридических лиц и субъектов квазигосударственного сектора.

Законодательством также не установлен запрет на приобретение государственными органами, государственными юридическими лицами и субъектами квазигосударственного сектора продуктов цифровых данных вне пределов платформ обмена и оборота продуктов цифровых данных.

При этом, Правилами функционирования платформ поставщики продуктов цифровых данных из числа субъектов частного предпринимательства на добровольной основе подтверждают качество своих продуктов цифровых данных на соответствие требованиям по управлению цифровыми данными (п. 13).

Указанное положение демонстрирует, что одной из **основных задач закрепления в Цифровом кодексе комплекса положений, регулирующих оборот продуктов цифровых данных на специализированных платформах, является формирование не только нового рынка продуктов цифровых данных, но и доверия к такому рынку.** Экономическая ценность продукта цифровых данных, как было указано, определяется не только содержанием данных, но и информацией об их происхождении, структуре, качестве, и условиях использования. Поэтому Цифровым кодексом и Правилами функционирования платформ устанавливаются специальные требования функционирования платформ, а также система контроля за исполнением таких требований.

4. Основной целью внедрения в Цифровой кодекс специальных положений в отношении продуктов цифровых данных и регламентации деятельности платформ обмена и оборота продуктов цифровых данных заключается в закреплении правовых основ для формирования рынка продуктов цифровых данных и выработки единых правил их обращения.

Пунктом 3 статьи 30 Цифрового кодекса установлено: *«Продукт цифровых данных на платформе обмена и оборота продуктов цифровых данных может быть предметом сделок, отчуждения и передачи на условиях, определенных владельцем, за исключением общедоступной информации, предусмотренной законодательством Республики Казахстан»*. Подробный комментарий относительно особенностей цифровых данных как объектов гражданского оборота смотрите к статьям 1 и 20 Цифрового кодекса.

Признание цифровых данных и цифровых объектов объектами гражданского оборота неизбежно вызывает вопрос об определении их стоимости. Цифровой кодекс практически не содержит таких специальных положений. Исключение составляют нормы статьи 31, предусматривающие разработку типовой методики оценки стоимости продуктов цифровых данных.

Цифровые данные, как было многократно указано в комментариях к разным статьям Цифрового кодекса, являются основным экономическим ресурсом такой составляющей цифровой экономики как экономика данных. Именно поэтому формирование рынка продуктов цифровых данных невозможно без разработки методологий и методик определения их стоимости. При этом, обоснованное определение стоимости следует рассматривать не только как инструмент ценообразования, но и как основу защиты интересов участников гражданского оборота.

Актуальность вопросов оценки данных подтверждается и международной практикой. В 2024 году Конференцией европейских статистиков (CES) в рамках Европейского экономического совета ООН (UNECE) совместно с Eurostat и МВФ разработан документ ООН «Handbook on the capitalisation of Data in the System of National Accounts»⁵¹. Документ определяет данные как новый класс активов, подлежащий оценке и учету. Данный подход имеет значение для развития механизмов оценки стоимости продуктов цифровых данных и формирования экономики

⁵¹ Handbook on the capitalisation of Data in the System of National Accounts / Conference of European Statisticians (CES), Group of Experts on National Accounts, Eurostat, International Monetary Fund (IMF). – Geneva: UNECE, 2024. // URL: https://unece.org/sites/default/files/2024-04/12_Handbook%20on%20the%20capitalisation%20of%20Data%20in%20the%20System%20National%20Accounts%20_outline_0.pdf (Дата обращения: 18.06.2026)

данных. Для Казахстана этот документ имеет рекомендательный статус как для страны-участницы ООН.

Как отмечается в документе, концептуально данные рассматриваются в качестве самостоятельного актива наряду с объектами интеллектуальной собственности, такими как результаты научно-исследовательских работ и программное обеспечение. При этом, особенности создания и использования данных потребовали разработки специальных подходов к их учету и оценке.

В исследовании OECD Measuring the Value of Data and Data Flows⁵² данные рассматриваются как самостоятельный экономический актив, ценность которого определяется не только затратами на его создание, но прежде всего возможностью получения экономических выгод от его использования.

Приведенные международные документы демонстрируют не только значимость определения стоимости данных и их продуктов как объектов гражданского оборота, нового класса активов и экономического ресурса, но и необходимость формирования единообразных подходов к ценообразованию.

Пунктом 8 статьи 31 Кодекса определено, что оценка стоимости продуктов цифровых данных для государственных органов, государственных юридических лиц и субъектов квазигосударственного сектора определяется Типовой методикой.

В соответствии с Типовой методикой продукты цифровых данных признаются государством новым видом нематериальных активов, обладающих самостоятельной имущественной ценностью, стоимость которой должна определяться с учетом востребованности на рынке, уникальности и затрат на создание.

Вместе с тем следует отметить, что Типовая методика ориентирована на государственный и квазигосударственный сектор и не устанавливает универсальных правил оценки для всех участников рынка данных. Однако сам факт признания государством продуктов цифровых данных самостоятельным активом создает предпосылки для формирования единых подходов к их коммерциализации и для частных субъектов.

Важно отметить, что Типовая методика не определяет минимальных и максимальных порогов ценообразования продуктов данных, соответственно, введение государственного регулирования цен на продукты цифровых данных не устанавливается.

⁵² Measuring the Value of Data and Data Flows / Organisation for Economic Co-operation and Development (OECD). – Paris: OECD Publishing, 2024. // URL: https://www.oecd.org/en/publications/measuring-the-value-of-data-and-data-flows_923230a6-en.html (Дата обращения: 18.06.2026)

Исходя из изложенного, можно сделать вывод, что **общемировой тенденцией является признание цифровых данных и продуктов их переработки как самостоятельного вида нематериальных активов, которые могут быть объектом гражданского оборота, учитываться при оценке имущественных вкладов в капитал компаний и использоваться при осуществлении инвестиционной деятельности.**

4. Цифровым кодексом устанавливается, что деятельность платформ по обмену и обороту цифровых данных является объектом контроля и надзора со стороны государства. Такой подход обусловлен, прежде всего, ролью самих платформ в процессе становления и развития рынка продуктов цифровых данных, а также спецификой продуктов цифровых данных как особого объекта гражданского оборота.

Статья 31 Цифрового кодекса и принятые во исполнение пункта 2 указанной статьи Правила функционирования платформ устанавливают следующие меры государственного контроля и надзора:

- 1) уведомление уполномоченного органа при начале или прекращении деятельности платформы.
- 2) внесение уполномоченным органом данных о платформе в реестр;
- 3) мониторинг уполномоченным органом деятельности собственников (владельцев) платформ.

Важно отметить, что уведомительный порядок входа на рынок продуктов цифровых данных в целом соответствует принципу свободы создания и применения цифровых технологий, установленному статьей 8 Цифрового кодекса. Государство не устанавливает требований относительно допуска на рынок.

Ведение специального реестра платформ обмена и оборота продуктов цифровых данных направлено на обеспечение прозрачности рынка продуктов цифровых данных и состав его участников. Наличие реестра позволяет государству определить круг субъектов, осуществляющих деятельность по организации оборота продуктов цифровых данных, получать информацию о масштабах рынка, а также обеспечивать применение единых требований к деятельности платформ.

Мониторинг платформ обмена и оборота продуктов цифровых данных со стороны уполномоченного органа осуществляется в отношении обязанностей собственников (владельцев) платформ, предусмотренных пунктом 5 статьи 31:

- 1) обеспечения создания и ведения перечня продуктов цифровых данных;

2) обеспечения условий доступа, обмена и использования продуктов цифровых данных;

3) предотвращения несанкционированный доступ, утечку и трансграничную передачу продуктов цифровых данных, если такая передача ограничена законами Республики Казахстан,

4) исполнения требований законодательства в сфере цифровизации, кибербезопасности, защиты персональных данных, а также правил функционирования платформ обмена и оборота продуктов данных.

Кроме этого, посредством мониторинга осуществляется сбор, оценка и анализ информации о состоянии, развитии, рисках обмена и оборота продуктов цифровых данных на платформе.

Завершая комментарий, важно отметить, что статьи 30 и 31 Цифрового кодекса являются одними из первых норм казахстанского законодательства, направленных на формирование правовых основ экономики данных. Кроме того, что Кодексом цифровые данные признаны объектом права и гражданского оборота, им также определены основы экономического использования продуктов переработки цифровых данных и ключевые условия их оборота и обмена на специализированных платформах.

Представляется вероятным, что по мере развития рынка продуктов цифровых данных будет осуществляться дальнейшая детализация правового регулирования вопросов их оценки, качества, использования и оборота, также совершенствование требований к функционированию платформ обмена и оборота продуктов цифровых данных.

РАЗДЕЛ 3. СУБЪЕКТЫ ЦИФРОВОЙ СРЕДЫ

Глава 7. СУБЪЕКТЫ ЦИФРОВОЙ СРЕДЫ, ИХ ВИДЫ, ПРАВА И ОБЯЗАННОСТИ

Статья 39. Пользователи цифровых объектов

1. Пользователями цифровых объектов признаются физические или юридические лица, которые на законных основаниях используют цифровые объекты в соответствии с пунктом 2 настоящей статьи.

2. Пользователь цифрового объекта вправе:

1) использовать цифровые объекты на условиях, определенных законодательством Республики Казахстан, собственником и (или) владельцем цифрового объекта;

2) получать достоверную информацию о характеристиках и рисках цифрового объекта;

3) защищать свои права от неправомерного ограничения доступа или злоупотреблений со стороны собственника и (или) владельца или иных пользователей цифрового объекта;

4) пользоваться иными правами, установленными настоящим Кодексом и законами Республики Казахстан.

3. Пользователь цифровых объектов обязан:

1) соблюдать требования [законодательства](#) Республики Казахстан по защите персональных данных и конфиденциальной информации;

2) не вмешиваться в функционирование цифрового объекта и не изменять его без разрешения собственника и (или) владельца цифрового объекта;

3) действовать добросовестно и не причинять вред другим пользователям цифрового объекта;

4) выполнять иные обязанности в соответствии с настоящим Кодексом и иными законами Республики Казахстан.

1. Статьей 39 Цифрового кодекса определяет правовой статус пользователей цифровых объектов как самостоятельной категории субъектов цифровой среды наряду с субъектами цифровых данных, а также собственниками и владельцами цифровых объектов, что следует из статьи 36 Цифрового кодекса.

Закрепление специального правового статуса пользователей цифровых объектов способствует реализации таких принципов правового регулирования отношений в цифровой среде, как: защита прав и свобод человека в цифровой среде, свободное и осознанное волеизъявление, а также обеспечение баланса интересов субъектов цифровой среды.

Отдельные права и обязанности пользователей цифровых объектов в аспекте особенностей доступа и пользования цифровыми объектами могут быть установлены иными законодательными актами.

Выделение пользователей цифровых объектов в самостоятельную категорию субъектов цифровой среды обусловлено тем, что в цифровой экономике многие лица не обладают правами на цифровые объекты, но постоянно используют их функциональные возможности.

Вместе с тем отсутствие прав на цифровой объект не означает отсутствия правового статуса. Пользователи должны обладать правами для защиты своих законных интересов в цифровой среде, а также осознавать и соблюдать установленные законодательством и правилами пользования обязанности.

Пункт 1 статьи определяет пользователей цифровых объектов как физических или юридических лиц, которые на законных основаниях используют цифровые объекты.

Из приведенного определения следует, что для признания лица пользователем цифрового объекта значение имеет не наличие у него прав на соответствующий объект, а факт его правомерного использования.

При этом **использование цифрового объекта предполагает использование не самого объекта как такового, а предоставляемых им функциональных возможностей.** Пользователь взаимодействует с цифровым объектом в целях получения доступа к определенным данным, сервисам, совершения операций, заключения сделок и т.д.

Именно поэтому Цифровой кодекс закрепляет функциональный статус пользователя, отличая его как от собственников и владельцев цифровых объектов, так и от потребителей товаров и услуг, которые могут использовать цифровые объекты лишь как средство получения соответствующих товаров, работ или услуг (например, интернет-магазины, маркетплейсы, стриминговые платформы и иные цифровые сервисы).

Проблемным представляется вопрос относительно приведенного определения пользователя и наличием у пользователей контроля над личными кабинетами и аккаунтами на цифровых объектах. Развитие этого вопроса в доктрине цифрового права может повлечь дополнительной регламентации правового статуса пользователя цифровых объектов.

2. В аспекте гражданского права статья 39 Цифрового кодекса определяет правовой статус пользователей цифровых объектов как самостоятельной категории субъектов цифровой среды. В отличие от собственников и владельцев цифровых объектов, пользователи не осуществляют правомочия собственника (владельца) в отношении таких объектов, а используют их на установленных условиях. Пользователь заинтересован, прежде всего, в доступе к цифровому объекту и использованию его функциональных возможностей.

Право пользования цифровыми объектами имеет особенности в связи с тем, что оно ограничено функциональными возможностями самого объекта, а также условиями пользования, установленными собственниками (владельцами) и законодательством. Поскольку может изменяться функционал цифровых объектов, могут изменяться и возможности их использования.

3. Пункт 1 статьи 39 устанавливает, что пользователями цифровых объектов признаются лица, использующие такие объекты на законных основаниях. Требование о наличии законных оснований пользования цифровым объектом означает, что доступ к нему и его использование должны осуществляться в соответствии с законодательством Республики Казахстан, а также условиями, установленными собственником или владельцем цифрового объекта.

Особое значение в рамках цифровой среды приобретает категория доступа к цифровому объекту. В отличие от традиционных объектов гражданских прав, возможность использования цифрового объекта во многом зависит именно от наличия доступа к его функциональным возможностям.

Право на доступ к цифровым объектам, в особенности к интернет-ресурсам, приобретает самостоятельное правовое значение и выступает необходимым условием реализации многих прав и законных интересов участников цифровой среды.

Право на доступ к различным элементам цифровой среды, включая право на доступ к сети Интернет, данным, информации в научных

дискуссиях⁵³ и на уровне актов международных организаций^{54,55} постепенно формируется как самостоятельный правовой режим, а не просто как предоставление технологической возможности пользования элементами цифровой среды.

Цифровой кодекс не содержит структурно выделенного блока норм, регламентирующих права доступа к различным элементам цифровой среды (объектам, данным, информации, услугам). Закрепление прав доступа, включая доступ к сети Интернет, в качестве прав пользователей, либо в более широком смысле – в качестве прав человека, требует их концептуального анализа и классификации на уровне научной доктрины.

4. Право на доступ к цифровому объекту реализуется в двух взаимосвязанных аспектах. Во-первых, оно предполагает наличие у пользователя возможности получить доступ к цифровому объекту, включая наличие технической возможности и допуск со стороны собственника или владельца объекта. Во-вторых, реализация права доступа зависит от совершения самим пользователем действий, необходимых для получения такого доступа, включая прохождение идентификации, аутентификации, регистрацию, предоставление необходимых сведений либо выполнение иных установленных требований. Только при наличии двух указанных элементов право доступа может быть реализовано в полном объеме.

При этом условия предоставления доступа должны быть понятными и заранее известными пользователю, что обеспечивает реализацию принципа свободного и осознанного волеизъявления в цифровой среде, закрепленного статьей 5 Цифрового кодекса.

Право доступа не является абсолютным. Условия предоставления, ограничения или прекращения доступа, как указано в подпункте 1) пункта 2 комментируемой статьи, могут определяться законодательством, а также собственником (владельцем) цифрового объекта.

Соответственно, необоснованное непредоставление доступа пользователю к цифровому объекту со стороны собственника (владельца), если такой доступ предусмотрен законодательством или пользовательским

⁵³ UN: Human Rights Council adopts resolution on human rights on the Internet. [Электронный ресурс]. URL: <https://www.article19.org/resources/un-human-rights-council-adopts-resolution-on-human-rights-on-the-internet/> (дата обращения: 26.03.2026)

⁵⁴ Бакунина З.А., Очиров Г.М. Конституционное право на доступ в Интернет: продолжающаяся дискуссия. Уральский журнал правовых исследований. 2021. № 4. С. 3–9. [Электронный ресурс]. URL: <https://cyberleninka.ru/article/n/konstitutsionnoe-pravo-na-dostup-v-internet-prodolzhayushchayasya-diskussiya> (дата обращения: 11.06.2026)

⁵⁵ Мочалов А.Н., Колобаева Н.Е., Несмеянова С.Э. Право на доступ в интернет: юридическое содержание и механизм реализации. Антиномии. 2021. Т. 21, вып. 3. С. 135–163. [Электронный ресурс]. URL: <https://cyberleninka.ru/article/n/pravo-na-dostup-v-internet-yuridicheskoe-soderzhanie-i-mehanizm-realizatsii/viewer> (дата обращения: 11.06.2026)

соглашением, может рассматриваться как ограничение права пользователя либо, в отдельных случаях как нарушение принципа равенства субъектов цифровой среды.

В свою очередь, несоблюдение пользователем установленного порядка получения доступа может квалифицироваться как несанкционированный доступ к объекту.

При этом **право на доступ не означает право на одинаковые условия доступа для всех пользователей.** В зависимости от назначения цифрового объекта, характера обрабатываемых данных, требований безопасности или иных обстоятельств доступ может носить дифференцированный характер и предусматривать специальные требования к пользователям.

Так, пункт 2 статьи 10 Кодекса устанавливает требование к разработке цифровых объектов, требования по доступности к которым установлены законодательством, с учетом доступности для лиц с инвалидностью, нарушениями зрения, слуха, речи и другими функциональными ограничениями и лиц, относящихся к маломобильным группам населения.

5. Пункты 2 и 3 статьи 39 регламентируют права и обязанности пользователей цифровых объектов. При их толковании следует учитывать, что данные нормы направлены не на детальную регламентацию поведения пользователей, а в большей степени на закрепление базовых прав и принципов пользования цифровыми объектами. Перечни прав и обязанностей носят открытый характер и предусматривают возможность установления дополнительных прав и обязанностей Цифровым кодексом и законами.

При этом, права пользователей цифровых объектов тесно связаны с обязанностями собственников и владельцев цифровых объектов, предусмотренными статьей 38 Цифрового кодекса. Реализация прав пользователей во многом зависит от надлежащего исполнения собственниками и владельцами соответствующих обязанностей.

Подпункт 2) пункта 2 статьи 39 предусматривает право пользователя на получение информации об условиях использования цифрового объекта. **Реализация данного права предполагает, одновременно, и ознакомление пользователя с такими условиями до начала использования объекта.** Используя цифровой объект, пользователь соглашается соблюдать требования законодательства и установленные правила пользования.

Такое положение обеспечивает реализацию принципа свободного и осознанного волеизъявления в цифровой среде, предусмотренного статьей 5 Цифрового кодекса, поскольку пользователь должен иметь возможность

заранее ознакомиться с условиями и ограничениями использования цифрового объекта.

6. Подпункт 3) пункта 2 статьи 39 закрепляет право пользователя защищать свои права от **неправомерного ограничения доступа или злоупотреблений со стороны владельца (собственника) объекта или иных пользователей цифрового объекта.**

Подпунктом 1) пункта 2 статьи 39 установлено, что условия использования цифровых объектов могут определяться законодательством или собственником (владельцем) цифрового объекта. Соответственно, неправомерность ограничения доступа означает нарушение таких установленных условий со стороны собственника (владельца), либо применение ограничений, не предусмотренных законодательством или правилами использования цифрового объекта.

Вместе с тем право пользователя на защиту не ограничивается случаями неправомерного ограничения доступа. Пользователь вправе защищать свои права и законные интересы также в случаях злоупотребления со стороны собственника (владельца) цифрового объекта или иных пользователей, если такие действия препятствуют использованию цифрового объекта либо нарушают права пользователя.

Право на защиту предполагает возможность использования пользователем предусмотренных законодательством способов защиты своих прав и законных интересов. В зависимости от характера нарушения пользователь может обратиться к собственнику или владельцу цифрового объекта, в уполномоченный государственный орган либо в суд.

7. Пункт 3 статьи 39 устанавливает основные обязанности пользователей цифровых объектов. Их закрепление направлено на обеспечение безопасного и добросовестного использования цифровых объектов, а также соблюдение прав и законных интересов других субъектов цифровой среды.

Подпункт 1) пункта 3 возлагает на пользователей обязанность соблюдать требования законодательства Республики Казахстан по защите персональных данных и конфиденциальной информации. В процессе использования цифровых объектов пользователи могут получать доступ к персональным данным, коммерческой тайне, служебной информации и иным сведениям ограниченного доступа. Использование такой информации должно осуществляться в соответствии с требованиями законодательства и правами лиц, которых она касается.

Подпункт 2) запрещает пользователям вмешиваться в функционирование цифрового объекта и изменять его без разрешения собственника или владельца. Цифровой объект представляет собой единый

технологический комплекс, стабильность и безопасность функционирования которого зависят от соблюдения установленных правил эксплуатации. Несанкционированное вмешательство может привести к нарушению работы цифрового объекта, повреждению данных, возникновению угроз информационной безопасности либо нарушению прав других пользователей.

Подпункт 3) закрепляет обязанность пользователя действовать добросовестно и не причинять вред другим пользователям цифрового объекта. Требование добросовестности является одним из базовых начал гражданского права и приобретает особое значение в цифровой среде, где действия одного пользователя цифрового объекта могут существенно затрагивать интересы значительного числа других лиц.

Указанная обязанность также соответствует принципу баланса интересов субъектов цифровой среды, закрепленному статьей 9 Цифрового кодекса, поскольку предполагает осуществление своих прав с учетом прав и законных интересов других участников цифровой среды.

Подпункт 4) пункта 3, а также подпункт 4) пункта 2 комментируемой статьи носят отсылочный характер и предусматривает возможность установления иных прав обязанностей пользователей цифровых объектов настоящим Кодексом и другими законами Республики Казахстан.