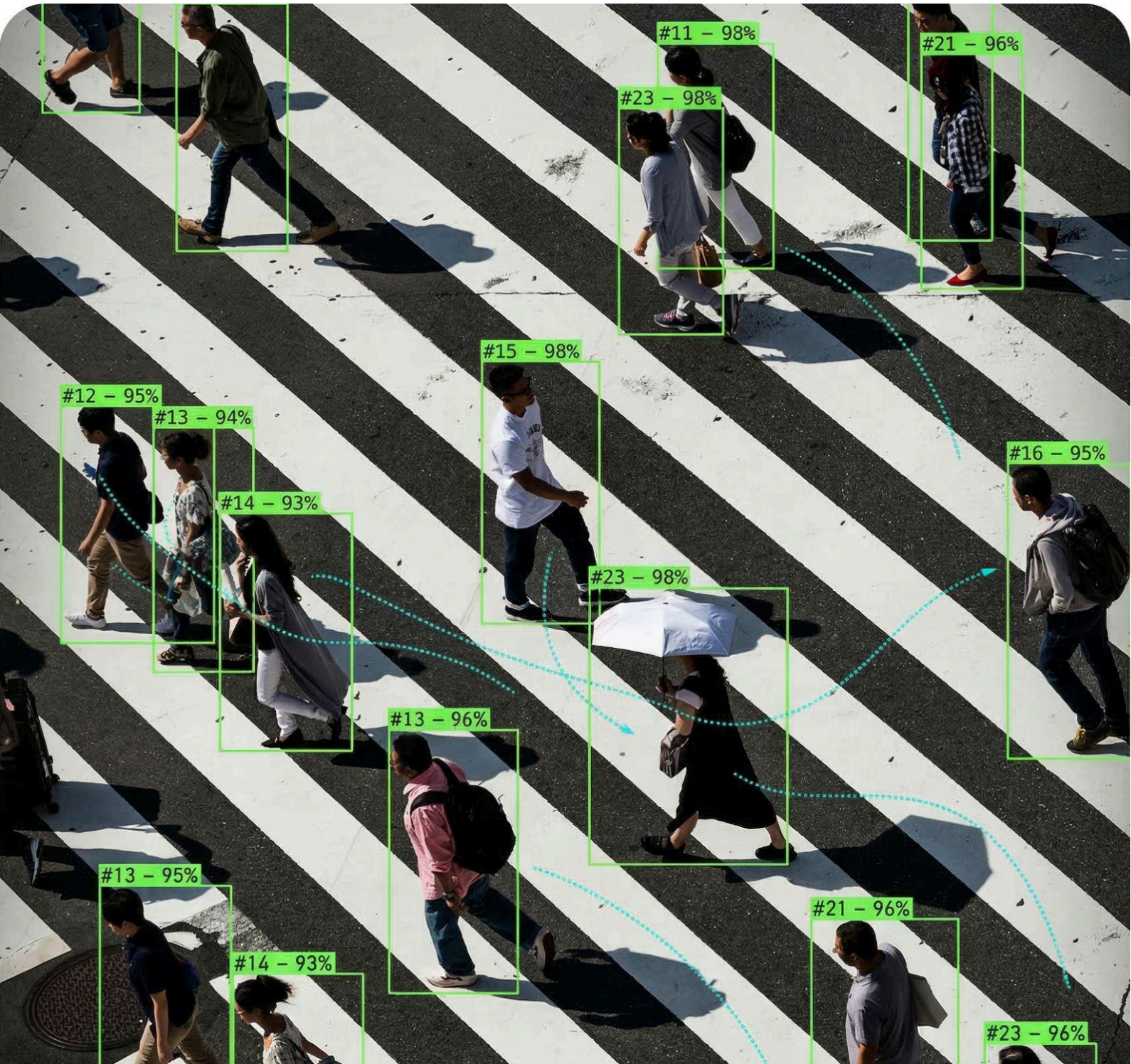
RKS Global

rks.global

Человек против модели: как государства используют ИИ для цензуры и слежки



Оглавление

Введение

Развитие современных систем и моделей ИИ связано в основном с частными компаниями и венчурным капиталом. Но государственные органы также стремятся участвовать в этой гонке, разрабатывать и использовать новые технологии для своих нужд. В ряде стран системы ИИ уже используются в правоохранительной деятельности, национальной обороне и обеспечении безопасности.

Во многих случаях внедрение систем ИИ позволяет ускорить работу государственного аппарата, повысить ее качество и снизить издержки. Автоматизация рутинных процессов, анализ больших массивов данных и прогнозирование социальных явлений открывают перед органами власти новые возможности для реализации государственных функций. Однако, положительные эффекты от применения ИИ неразрывно связаны с существенными рисками для прав и свобод человека. Системы распознавания лиц, автоматизированного мониторинга интернета и предиктивной аналитики могут быть использованы не только для противодействия преступности и обеспечения общественного порядка, но и для подавления политической оппозиции, преследования инакомыслящих и установления тотального контроля над населением.

В этом контексте особую тревогу вызывает ситуация в государствах с авторитарными и гибридными политическими режимами. Отсутствие независимой судебной системы, слабость институтов гражданского общества и ограниченная подотчетность органов власти создают условия, при которых возникает соблазн использовать новейшие технологии для удержания власти. Недостаточное правовое регулирование в сфере разработки и применения систем ИИ и отсутствие механизмов обеспечения прозрачности нередко маскируются риторикой о необходимости стимулирования инноваций и поддержки технологического бизнеса. Дополнительным фактором выступает конкуренция между ведущими технологическими державами, которые стремятся распространить

своё влияние в том числе посредством экспорта систем наблюдения и цифровой инфраструктуры.

Основной целью этого исследования является изучение текущего состояния нормативного регулирования в сфере разработки и применения систем ИИ в отдельных странах Евразии, анализ государственных инвестиций в технологическое развитие, а также систематизация имеющейся информации о возможностях использования систем ИИ для осуществления онлайн-цензуры, гласного и негласного наблюдения.

Исследование основано на анализе открытой информации: нормативных правовых актов, официальных документов стратегического планирования, отчетов международных и правозащитных организаций, материалов СМИ и академических публикаций. Кроме того, были проведены интервью с экспертами, которые обладают практическим знанием о практике применения систем ИИ в соответствующих юрисдикциях.

Азербайджан

Концепции и нормативное правовое регулирование

Основным концептуальным документом является Стратегия развития ИИ на 2025-2028 годы. Она определяет пять ключевых направлений, одним из которых является разработка нормативного правового регулирования в сфере ИИ. Сегодня ведется дискуссия относительно содержания будущего регулирования, а заинтересованные стороны представляют свои проекты.

В рамках регулирования в сфере цифровых технологий предполагается в дальнейшем внести изменения в Закон “О персональных данных”.

В январе 2025 года утверждена Концепция цифрового развития, направленная на ускорение экономического развития через цифровые технологии.

При Министерстве экономики функционирует Центр Четвертой промышленной революции (Center for Analysis and Coordination of the Fourth Industrial Revolution, C4IR), который осуществляет координацию и анализ инициатив и проектов в сфере цифровой экономики.

Финансирование и стратегические проекты

Во многом развитие сферы ИИ предполагается за счет предоставления средств частным компаниям и государственным органам. Агентство по инновациям и цифровому развитию (Innovation and Digital Development Agency, IDDA) координирует цифровую трансформацию страны и поддержку стартап-экосистемы. ASAN AI Hub координирует сотрудничество между государственным

сектором, бизнесом, исследовательскими центрами и стартап-экосистемой в сфере ИИ.

В декабре 2024 года Европейский инвестиционный банк предоставил заем на 43 млн. евро на строительство двух дата-центров уровня Tier 3.

Применение систем ИИ для цензуры

В Азербайджане органы власти вправе потребовать удалить противоправный контент или ограничить доступ к интернет-ресурсу в соответствии со статьей 13.3 Закона "Об информации, информатизации и защите информации". Если провайдер не выполнил требования регулятора, то ограничить доступ может суд. В срочных случаях доступ может быть ограничен по решению органов исполнительной власти с последующим судебным рассмотрением. Однако, черный список ресурсов, к которым ограничен доступ, не доступен публично. Деятельность органов власти носит достаточно закрытый характер, что не позволяет оценить, применяются ли системы ИИ для поиска противоправного контента.

В соответствии со статьей 10 Закона "Об оперативно-розыскной деятельности", прослушивание телефонных переговоров и извлечение информации из каналов связи не требует судебного санкционирования или контроля вышестоящего органа, если не предполагается установка технических устройств в жилище. Freedom House в 2023 году указывал, что, вероятно, используются технические средства системы оперативно-розыскных мероприятий (СОРМ) с применением технологии глубокой инспекции пакетов (DPI).

Азербайджан систематически блокирует независимые СМИ и ограничивает доступ к социальным сетям, особенно во время чрезвычайных ситуаций. Например, в периоды конфликтов и протестов блокировался доступ к отдельным интернет ресурсам и социальным сетям.

Применение систем ИИ для гласного и негласного наблюдения

Установка видеонаблюдения в Азербайджане осуществляется в рамках проекта “Безопасный город”. По данным за 2023 год, в стране установлено около 15 тыс. камер. С юридической точки зрения идентификация осуществляется в соответствии с Законом “О биометрической информации”. В ноябре 2025 года президентом был подписан указ о создании Централизованной системы информации и цифровой аналитики MIRAS, которая предполагает объединение баз данных разных органов власти для создания единого цифрового портфеля граждан. Human Rights Watch выразила обеспокоенность тем, что централизованная система, объединяющая чувствительные персональные данные из различных ведомств в отсутствие надлежащего независимого надзора, создает серьезные риски произвольной или непропорциональной слежки.

По данным правозащитных организаций, государственные органы неоднократно использовали шпионское ПО Pegasus. Например, по данным Amnesty International, на 2023 год более 1 тыс. азербайджанских номеров были выбраны для потенциального таргетирования клиентом Pegasus.

Армения

Концепции и нормативное правовое регулирование

Национальная стратегия развития ИИ в Армении находится на этапе разработки и обсуждения. Предполагается, что она в большей степени будет направлена на внедрение систем ИИ в отдельные сферы общественной жизни. К сфере ИИ применяется общее законодательство страны, отдельные законодательные решения пока не анонсированы.

Финансирование и стратегические проекты

В 2025 году анонсировано государственно-частное партнерство на 500 млн. долларов с компанией Firebird.ai на создание суперкомпьютерного дата-центра на базе технологий ИИ с предполагаемой мощностью в 100 мегаватт.

Также, в начале 2025 года было подписано соглашение о сотрудничестве как в частной, так и в государственной сферах с французским ИИ-стартапом Mistral AI.

Помимо этого, правительство осуществляет программы поддержки предпринимателей и стартапов в сфере ИИ.

Применение систем ИИ для цензуры

В соответствии с законодательством, операторы связи должны блокировать сайты, нарушающие законодательство (прежде всего, нелегальные казино и гэмблинг).

Точечные блокировки соцсетей применялись отдельными операторами связи во время вооруженного конфликта в 2020 году.

Применение систем ИИ для гласного и негласного наблюдения

В 2020 – 2022 годах ряд общественных деятелей подверглись взломам с использованием шпионского ПО Pegasus и Predator, однако конкретные заказчики не установлены. Косвенные улики указывают на применение Pegasus со стороны государственных органов Азербайджана, а Predator – Армении.

В 2025 году вступили в силу поправки в закон “О полиции”, которые для осуществления биометрической идентификации предоставили полиции доступ к камерам, расположенным в публичных местах.

С 2017 по 2018 годы в рамках проекта “Умный город” камеры и инфраструктура поставлялись китайскими компаниями, однако в последние годы наметился переход на сотрудничество с США и Индией.

Беларусь

Концепции и нормативное правовое регулирование

В Беларуси отсутствует специальное нормативное правовое регулирование в сфере ИИ, к отрасли применяются нормы общего законодательства. Предполагается, что концептуальные документы и нормативные правовые акты начнут разрабатывать в 2026 году.

В 2025 году утверждена Госпрограмма “Цифровая Беларусь” на 2026–2030 годы. В качестве ключевых направлений она определяет развитие государственных цифровых платформ и внедрение технологий обработки данных, включая ИИ.

В 2025 году рабочей группой ОИПИ НАН Беларуси разработан Модельный закон СНГ о технологиях искусственного интеллекта, который был принят Межпарламентской Ассамблеей СНГ. Сам документ представляет собой компиляцию отдельных положений Регламента ЕС по ИИ и Рамочной конвенции Совета Европы об искусственном интеллекте и правах человека, демократии и верховенстве права. Поскольку документ фактически нереализуем на практике, государства СНГ не имплементировали его в национальное законодательство.

В 2025 году также был создан комитет по стандартизации “Цифровое развитие и связь” (ТК DY 41). Предполагается, что он будет разрабатывать технические стандарты в сфере ИИ и координировать их соответствие российским и международным практикам.

Финансирование и стратегические проекты

Ключевым инструментом развития IT-сектора и технологий ИИ в стране остается Парк высоких технологий, основанный в 2005 году.

В стране реализованы несколько крупных ЦОД уровня Tier 3: Республиканский центр обработки данных (РЦОД) компании beCloud и ЦОД компании А1[1].

В 2025 году с представителями России обсуждался проект создания крупного ЦОД, который работал бы на атомной энергии.

Применение систем ИИ для цензуры

Ограничение доступа к контенту и интернет-ресурсам в Беларуси осуществляется на основе ст. 51[1] Закона "О средствах массовой информации", которой предусматривается возможность осуществления внесудебных блокировок по решению Министерства информации (и других органов) или постановлению прокуроров. Перечень запрещенного к распространению информации содержится в ст. 38.

Вторым законом, на основании которого осуществляется цензурирование интернета, является Закон "О противодействии экстремизму". Он разрешает как ограничение доступа к отдельным ресурсам в административном порядке, так и признание материалов и организаций экстремистскими – в судебном.

Всего в стране экстремистскими было признано более 6,3 тысяч интернет-ресурсов, а заблокировано – более 18 тыс.

Полномочия органов власти дополнительно расширяются за счет принятия новых подзаконных актов. Например, в сентябре 2025 года отдельным постановлением Совета министров предусмотрена возможность отключения отдельных абонентов от сотовой связи и интернета.

Практика ограничения доступа к интернету или отдельным ресурсам в масштабах страны применялась в период массовых протестов в августе 2020 года и в ходе президентских выборов в январе 2025 года. Если в 2020 году было фактически зафиксировано полное

---

[1] Прим.: сайт https://a1digital.by/ на момент провдения исследования не функционирует.

отключение интернета, то в 2025 году ограничения носили более селективный характер и проявлялись в виде перебоев доступа к отдельным платформам. По некоторым данным, в 2020 году при блокировках использовались технологии глубокой инспекции пакетов (DPI).

Несмотря на то, что публично информация о применении систем ИИ при осуществлении интернет-цензуры в Беларуси не публикуется, масштаб и скорость блокировок объективно предполагают использование автоматизированных средств мониторинга и обработки информации. При этом, отсутствие специального правового регулирования открывает для государственных органов возможности по скрытому использованию систем ИИ, что затрудняет оценку реальных масштабов применения таких технологий.

Применение систем ИИ для гласного и негласного наблюдения

Правовую основу использования разнообразных систем наблюдения государственными органами составляет Закон "Об оперативно-розыскной деятельности". В 2014 году был издан указ президента "О вопросах создания и применения системы видеонаблюдения в интересах обеспечения общественного порядка". Он определяет ответственные органы и порядок установки оборудования.

Центральным элементом системы видеонаблюдения в Беларуси является платформа Kipod, разработанная белорусской компанией Synesis. Платформа основана на применении систем ИИ для обеспечения контроля за совершением правонарушений и перемещений людей и транспортных средств.

По данным МВД, в 2025 году в стране действует более 60 тыс. камер, которые подключены к единой платформе с применением технологий Kipod.

В 2010 году был издан указ президента “О мерах по совершенствованию использования национального сегмента сети Интернет”. Он регламентирует установку инфраструктуры СОРМ по российской модели. Технические характеристики оборудования были определены в 2023 году отдельным документом.

В декабре 2025 года журналисты сообщили об обнаружении ранее неизвестного шпионского ПО ResidentBat, используемого белорусскими спецслужбами для слежки за журналистами.

Грузия

Концепции и нормативное правовое регулирование

Национальная стратегия развития ИИ в Грузии находится на этапе разработки и обсуждения. К сфере ИИ применяется общее законодательство страны.

В 2024 году Грузия подписала Рамочную конвенцию Совета Европы об искусственном интеллекте и правах человека, демократии и верховенстве права, в рамках которой предусматривается, что государства берут на себя обязательства по снижению рисков для прав человека, демократии и верховенства права, потенциально возникающих на всех стадиях жизненного цикла систем ИИ.[2] Предполагается, что дальнейшие шаги по нормативному правовому регулированию будут соответствовать духу Конвенции СЕ и подходу ЕС.

Финансирование и стратегические проекты

Финансирование сферы ИИ включено в общие расходы на цифровое развитие. Прямое финансирование осуществляется главным образом через поддержку стартапов Агентством по инновациям и технологиям Грузии (Georgia's Innovation and Technology Agency, GITA), которое выделило ИИ как один из трех ключевых технологических приоритетов страны. Постепенно системы ИИ внедряются в различные сферы — образование, здравоохранение, финансы.

---

[2] Прим.: Рамочная конвенция пока что не вступила в силу, так как на момент подготовки отчета не была ратифицирована необходимым числом стран.

Применение систем ИИ для цензуры

Национальная комиссия по коммуникациям Грузии (The Georgian National Communications Commission, ComCom) осуществляет блокировки сайтов, нарушающих законодательство страны (нарушение авторских прав, гэмблинг, порнография), однако единый черный список запрещенного контента и интернет-ресурсов не ведется.

В целом использование систем ИИ для блокировки контента находится на начальном уровне, однако законы о запрете пропаганды ЛГБТ+, об иностранных агентах и оскорблении власти открывают широкие возможности по модерации контента.

В 2023 году компания Meta удалила сеть из 117 аккаунтов, которая осуществляла размещение информации в поддержку государственной власти и критиковала оппозицию во время протестов. Meta связала данную сеть с государственными органами Грузии.

Применение систем ИИ для гласного и негласного наблюдения

За последние годы в Грузии были установлены более 4 тыс. “умных” камер и иной инфраструктуры японских, китайских и российских производителей (NEC, Hikvision, Dahua and Papillon Systems).

В 2024 году изменения законодательства сначала позволили ввести запрет на закрытие лиц, использование пиротехники и лазеров во время публичных мероприятий. В 2025 году биометрическая идентификацию для поиска лиц, совершивших административные правонарушения, была также легализована через законодательные изменения. Тем не менее, законы и подзаконные акты не регулируют процессуальные гарантии применения этих технологий — это остается на откуп правоохранительным органам без должных мер по раскрытию информации для общественности.

Правозащитники отмечают, что камеры с использованием технологии распознавания лиц массово применялись в ходе протестов в 2024 – 2025 годах и привели к выставлению штрафов за перекрытие улиц на более чем 730 тыс. долларов США.

Казахстан

Концепции и нормативное правовое регулирование

Основным стратегическим документом является Концепция развития ИИ на 2024 – 2029 годы. Документ определяет необходимость принятия дополнительных актов, которые обеспечат безопасное и этическое использование новых технологий. Вместе с тем отмечается, что часть смежных со сферой ИИ отношений планируется урегулировать в рамках Концепции цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023 – 2029 годы.

В начале 2026 года вступил в силу Закон "Об искусственном интеллекте", который регулирует отношения в сфере разработки и применения систем ИИ. Закон устанавливает семь запрещенных ИИ-практик, а также подразделяет оставшиеся системы ИИ на три группы по уровню риска для безопасности пользователей, общества и государства: высокий, средний и минимальный. Среди запрещенных практик выделяются такие как:

- манипуляции уязвимости отдельных социальных групп,
- социальная или биометрическая классификация в целях дискриминации,
- определение эмоций без согласия,
- нарушение законодательства о персональных данных,
- создание и распространение запрещенных законом материалов.

Также вводятся требования о маркировке синтетического контента. Вместе с тем, Документ хоть и исходит из риск-ориентированного подхода аналогично Регламенту ЕС по ИИ, но в текущем виде скорее

является основой, которая будет конкретизирована подзаконными актами. Например, выделяются требования для пользователей и владельцев систем ИИ. Однако, они почти никак не связаны с дифференциацией систем ИИ по группам риска.

Для реализации государственной политики в сентябре 2025 года создано Министерство искусственного интеллекта и цифрового развития. Также, в середине 2026 года вступит в силу новый Цифровой кодекс, который устанавливает комплексное регулирование для сферы информационных технологий.

Финансирование и стратегические проекты

По информации, содержащейся в Концепции развития ИИ, в Казахстане уже функционируют 51 ЦОД, 15 ЦОД принадлежат оператору инфраструктуры электронного правительства. Также, на базе исследовательских учреждений будт созданы несколько суперкомпьютеров разной мощности.

В марте 2025 года подписано соглашение с сингапурской компанией GK Hyperscale Ltd на строительства ЦОДов уровня Tier 3. Привлечены инвестиции на сумму 1,5 млрд. долларов.

В июле 2025 года казахстанская компания Akashi Data Center и китайская телекоммуникационная компания China Mobile подписали меморандум о сотрудничестве по созданию крупнейшего в Центральной Азии ЦОД уровня Tier 4.

В июле 2025 года в Астане запущен суперкомпьютерный центр Alem.cloud, который является самым мощным суперкомпьютером в Центральной Азии производительностью около 2 экзафлопс. Суперкомпьютер создан в партнерстве с эмиратской компанией Presight.

В 2024 и 2025 годах были выпущены несколько дообученных на наборах данных на Казахском языке моделей ИИ на базе модели Llama от Meta: KazLLM и Sherkala (8B). Также была создана

собственная большая языковая модель AlemLLM и мультимодальная модель Oylan. В 2025 году объявлено о сотрудничестве компаний Telegram с суперкомпьютерным кластером Казахстана по реализации проектов на стыке ИИ-технологий и блокчейна.

Для развития ИИ-экосистемы создан Национальная платформа ИИ, обеспечивающую разработчиков доступом к высококачественным данным и вычислительным ресурсам в защищенной государственной сети и Международный центр ИИ Alem.AI.

Применение систем ИИ для цензуры

Правовой основой для блокировки контента и интернет-ресурсов служит Закон Республики Казахстан «О национальной безопасности», который позволяет государственным органам принудительно приостанавливать телекоммуникации в ходе антитеррористических операций или подавления массовых беспорядков.

Ст. 41-1 Закона “О связи” устанавливает административный порядок временного приостановления связи и блокировки интернет-ресурсов. По представлению Генерального прокурора, его заместителей или по срочному решению органов национальной безопасности операторы связи, онлайн-платформы и государственная техническая служба обязаны в течение двух часов ограничить работу сетей, услуг связи или доступ к контенту, если он используется в преступных целях. Предварительное судебное решение в таком случае не нужно, уведомление об ограничении посылается постфактум. После устранения нарушения предусмотрена возможность снятия ограничений.

В рамках данных полномочий с 2017 года был запущен проект Кибернадзор, которая представляет собой информационную систему, с помощью которой государственные органы взаимодействуют между собой для выявления и блокировки противоправного контента. С помощью информационной системы были заблокированы сотни тысяч интернет ссылок, а также более 38 тыс. интернет-ресурсов с противоправным контентом. Несмотря

на то, что применение систем ИИ в функционировании информационной системы прямо не указано, можно предположить, что с учетом количества заблокированной информации, автоматизированные решения могут применяться.

В рамка Закона “О противодействии экстремизму” в отношении распространения запрещенной информации может использоваться прокурорский надзор, а организация может быть признана экстремистской в судебном порядке. Аналогичные меры производятся также в рамках Закона “О противодействии терроризму”.

В соответствии со ст. 14 Закона “Об онлайн-платформах и онлайн-рекламе” собственник или законный представитель онлайн-платформы обязан удалить противоправный контент или ложную информацию о человеке.

В январе 2022 года в ходе массовых протестов наблюдались отключения интернета и блокировки мессенджеров в течение недели.

Применение систем ИИ для гласного и негласного наблюдения

Видеонаблюдение в публичных местах осуществляется на основе Закона “Об оперативно-розыскной деятельности”. Однако применение систем ИИ отдельно не регулируется нормативными правовыми актами за исключением запрещенных практик, введенных Законом “Об искусственном интеллекте”.

По данным на 2025 год общая сеть видеонаблюдения насчитывает более 1,6 млн. камер. Из них 475 тыс. подключено к Центрам оперативного управления, а 20,5 тыс. – с системами ИИ. В большинстве своем используется инфраструктура китайских производителей Hikvision и Dahua Technology. В Казахстане разрабатываются и свои системы наблюдения. Например, ИИ-платформа TargetEYE.

Цифровой кодекс в ст. 48 предусматривает создание национальной системы биометрической аутентификации, которая станет ключевым инструментом для доступа к госуслугам, проведения проверок и защиты персональных данных. Необходимость передавать свои биометрические данные для граждан в стране постепенно расширяется на услуги разного рода. Например, с января 2026 года покупка SIM-карт в стране возможна только посредством передачи биометрических данных. Наличие единого центра хранения данных в руках государственных органов потенциально создает широкие возможности для слежки в реальном времени при помощи ИИ.

По данным журналистов, во время протестов 2022 года Китай направил в Казахстан специальную группу видеоаналитики для идентификации протестующих с помощью систем ИИ.

В стране также используется инфраструктура СОРМ с применением технологии глубокой инспекции пакетов (DPI). По данным журналистов, ранее использовались российские технологии, но в последние годы им на смену пришли комплексы и программное обеспечение китайских компаний (например, Geedge).

Кыргызстан

Концепции и нормативное правовое регулирование

В сентябре 2025 года появилась информация, что в стране разрабатывается и обсуждается будущая Концепция развития ИИ.Она будет направлена на определение стратегических целей развития отрасли.

В начале 2025 года был создан Национальный совет по развитию ИИ, который представляет собой совещательный орган по взаимодействию разных заинтересованных сторон.

С 2026 года начал действовать Цифровой кодекс, который представляет собой единый системный документ, направленный на регулирование в отношений в сфере информационных технологий. Ст. 16 Кодекса предусматривает полномочия президента страны по введению “специального регулирования”, что в дальнейшем может использоваться в качестве юридического обоснования внедрения репрессивных и ограничительных мер в том числе и в интернете.

Глава 23 Кодекса направлена напрямую на разработку и применение систем ИИ: устанавливаются требования для разработчиков и пользователей систем ИИ повышенного риска, а также требования по раскрытию информации. Несмотря на то, что концептуально данные положения схожи с требованиями к операторам систем ИИ повышенного риска в Регламенте ЕС, в большей степени их реализация будет определяться подзаконными актами.

Финансирование и стратегические проекты

В 2025 году объявлено о реализации проекта по закупке оборудования для дата центров на 2,5 млн. долларов, которые дополнят текущую инфраструктуру.

По данным СМИ, с 2023 года реализуется проект ИИ-ассистента Акылай (AkylAI), который архитектурно представляет собой модель Llama от Meta, обученную на наборе данных на кыргызском языке.[3] Также заявлено о том, что в рамках проекта будет создана умная колонка.

Применение систем ИИ для цензуры

Блокировки контента и интернет-ресурсов в судебном порядке осуществляются в соответствии с главой 25 ГПК, в которой устанавливается порядок ограничения доступа к террористическим или экстремистским материалам. Само понятие таких материалов и ограничения их распространения определяются Законом "О противодействии экстремистской деятельности". Отдельный черный список контента или интернет-ресурсов не опубликован. Однако, на сайтах операторах можно найти списки ресурсов, заблокированных по решению суда. Например, список оператора Мегалайн насчитывает более 200 записей.

В 2021 году был принят Закон Кыргызской Республики "О защите от ложной информации", предоставляющий частным лицам право требовать удаления онлайн-контента о себе, который они считают ложным, в течение 24 часов под угрозой приостановки работы сайта. По данным правозащитников, данный закон также используется в качестве внесудебного способа удаления контента и ограничения доступа к интернет-ресурсам.

В апреле 2024 года был заблокирован доступ к TikTok. Официальным основанием послужило несоблюдение Закона "О мерах по предотвращению вреда здоровью детей, их физическому, интеллектуальному, психическому, духовному и нравственному развитию", принятого в августе 2023 года. Правозащитники предупреждают, что данный закон может использоваться в качестве оснований для блокировок.

---

[3] Прим.: на момент подготовки исследования сайт https://www.akylai.com/ не функционирует.

В 2020 году, по данным журналистов, на парламентских выборах использовались “фабрики троллей”. В 2024 году были внесены изменения в Закон “О некоммерческих организациях”, которые добавили положения, созданные по принципу законодательства РФ об иностранных агентах.

Несмотря на то что в данный момент отсутствует информация об использовании систем ИИ для ограничения доступа к контенту и интернет-ресурсам, государственные органы обладают необходимыми юридическими механизмы по их внедрению без должных требований к прозрачности.

Применение систем ИИ для гласного и негласного наблюдения

Правовую основу использования видеонаблюдения составляют Закон “Об оперативно-розыскной деятельности” и Закон “О персональных данных”. Отдельных положений об обработке биометрических данных не содержится даже в новом Цифровом кодексе.

На 2025 год МВД заявляет о подключении около 25 тыс. видеокамер в рамках проекта “Безопасная страна”, включая камеры других ведомств, при этом часть из них использует распознавание лиц и интегрирована с базами МВД. Ранее в рамках проекта “Безопасный город” было установлено около 12 тыс. камер. Точные технические характеристики инфраструктуры публично не распространялись. На первых этапах построения системы наблюдения осуществлялось сотрудничество с китайскими компаниями CEIEC, Huawei и российской Vega.

В 2014 года принято постановление правительства, которое определяет порядок взаимодействия операторов мобильной сотовой связи с правоохранительными органами. Фактическим документ юридически закрепляет установку инфраструктуры СОРМ по образцу Российской Федерации.

Россия

Концепции и нормативное правовое регулирование

Основным концептуальным документом является Национальная стратегия развития искусственного интеллекта до 2030 года. Стратегия утверждена указом президента и является программным документом. Комплексная система нормативного правового регулирования в стране не разработана. Текущее нормативное регулирование касается лишь отдельных сфер, таких как оборот данных, медицина, транспорт.

В качестве ключевого регуляторного инструмента долгое время считались экспериментальные правовые режимы (ЭПР), правила создания которых утверждены федеральным законом. Отдельный экспериментальный режим, направленный прежде всего на упрощенный доступ к данным граждан, функционирует с 2020 года на территории Москвы.

Технический комитет № 164 активно разрабатывает свои и адаптирует международные стандарты в сфере ИИ, большая часть из которых являются рекомендательными.

Основная ставка делается на Кодекс этики в сфере ИИ и дополнительные документы к нему. Документ является добровольным и не содержит конкретных обязательств для субъектов, что позволяет ему создавать “фасад” нормативного регулирования при его содержательном отсутствии. Россия активно продвигает этот кодекс и за пределами страны.

Финансирование и стратегические проекты

Стратегия определяет, что к 2030 году мощность должна вырасти не менее чем до 1 экзафлопса по сравнению с 0,073 в 2022 году, а

объем затрат организаций на внедрение и использование технологий ИИ должен вырасти не менее чем до 850 млрд. рублей в год по сравнению со 123 млрд. рублей в 2022 году.

В рамках национального проекта “Экономика данных и цифровая трансформация государства” функционирует федеральный проект “Искусственный интеллект”. Общие расходы на 2025 – 2027 годы составят более 26 млрд. рублей. Весь национальный проект до 2030 года оценивается в 1 – 1,5 трлн. рублей без учета частных инвестиций в развитие отрасли.

Политическое руководство страны активно провозглашает курс на создание “суверенных” моделей ИИ, выходные результаты работы которых должны соответствовать законодательству и “традиционным ценностям”. На сегодняшний день в России есть две основные модели ИИ: YandexGPT и GigaChat. Обе из них разработаны аффилированными с государством компаниями Яндекс и Сбер (крупнейший банк). Другие частные компании либо находятся на этапе создания своих моделей ИИ, либо используют китайские (Qwen, DeepSeek, Kimi и д.р.). Тем не менее, развитие суверенных моделей тормозят жесткие санкции со стороны западных стран, ограничивающие поставки чипов, облачных ресурсов и моделей, а также недостаточность финансирования и кадров в условиях войны в Украине. Поставки оборудования, как правило, осуществляется нелегально с участием дружественных России стран.

Применение систем ИИ для цензуры

Несколько последних десятилетий в России постепенно выстраивается система тотального контроля государства над интернетом. Основным актом, определяющим порядок ограничения доступа к информации, является Закон “Об информации, информационных технологиях и о защите информации”. Документом устанавливается внесудебный и судебный порядок включения сетевых адресов и доменных имен в единый реестр. После включения ресурса в реестр владельцы сайтов, провайдеры хостинга и операторы связи должны предпринять необходимые

меры для удаления контента. По информации на начало 2026 года, в реестре содержится более 4,7 млн. записей.

В практике реализации блокировок в России применяется автоматизированная система “Ревизор”, разработанная Роскомнадзором и предназначенная для контроля исполнения операторами связи требований по ограничению доступа к запрещенной информации.

После принятия так называемого закона о “суверенном Рунете”, внесшему поправки в Закон “Об информации...” и Закон “О связи”, операторы связи стали обязаны устанавливать технические средства противодействия угрозам (ТСПУ) с применением технологий глубокой инспекции пакетов (DPI). Это позволило осуществлять массовые блокировки соцсетей, цифровых платформ и VPN-сервисов после 2022 года. Благодаря реализации информационной системы “Мир”, с 2024 года мониторинг сайтов осуществляется государственными органами с применением систем ИИ.

В архитектуре “суверенного Рунета” ключевую роль играет ЦМУ ССОП и одноименная информационная система мониторинга и управления сетью связи общего пользования, обеспечивающая централизованный контур наблюдения и управления

С 2023 года начала действовать информационная система “Окулус” для автоматизированного выявления запрещенного контента в интернете. В 2024 году появилась информация о регистрации информационной системы “Вепрь”, которая направлена на мониторинг интернета. Также была запущена система АС “Мавр”, которая направлена на поиск противоправного контента на стриминговых сервисах.

Россия активно использует системы ИИ и для дезинформации: в июле 2024 года Министерство юстиции США объявило о пресечении деятельности бот-фермы с применением систем ИИ для создания фиктивных профилей американцев в социальных сетях и распространения прокремлевских нарративов. Массово генерировались дипфейки в контексте войны в Украине и президентских выборов в США. Российские пропагандистские

материалы массово попадают в обучающие наборы данных для передовых моделей ИИ (ChatGPT-4, Grok, Mistral, Copilot, Meta AI, Claude, Google Gemini и др.), что влияет на содержание их выходных результатов.

Применение систем ИИ для гласного и негласного наблюдения

Основным документом, наделяющим государственные органы полномочиями по наблюдению, является Закон "Об оперативно-розыскной деятельности". По данным Минцифры, в России функционируют более 1 млн. камер. Крупнейшая сеть функционирует в Москве Она объединена с государственной информационной системой "Единый центр хранения и обработки данных (ЕЦХД)". Для беспрепятственного сбора персональных данных без согласия субъекта с 2020 года в соответствии с отдельным федеральным законом в Москве реализуется эксперимент, который направлен на развитие технологий ИИ. Основными поставщиками оборудования и ПО для наблюдения являются NtechLab, Tevian, VisionLabs и белорусская Synesis (Kipod). В рамках национального проекта "Экономика данных и цифровая трансформация государства" предполагается, что к 2030 году число камер видеонаблюдения в стране вырастет до 5 млн., все они будут объединены в единую информационную систему и снабжены системами ИИ для обработки видеопотока.

Важно отметить, что использование систем ИИ и иных цифровых технологий для осуществления гласного и негласного наблюдения не обеспечено нормативной правовой базой и фактически является произвольным для органов власти, что в частности было отдельно отмечено решением ЕСПЧ по делу Глухина против России.

Для осуществления идентификации и аутентификации в 2018 году была создана Единая биометрическая система, в которой хранятся все биометрические персональные данные. Предполагается, что в будущем биометрические данные всех лиц, находящихся на территории РФ, будут храниться в базе. Таким образом, государство

имеет как эксклюзивный доступ ко всем биометрическим данным, так и возможность определять, каким субъектам предоставить доступ к базе данных.

В 2024 году в Закон “О персональных данных” под предлогом необходимости создания механизма по обмену наборами данных для бизнеса для создания систем ИИ были внесены изменения (ст. 13.1), которые предполагают создания единой государственной системой по хранению таких данных.

С 1996 года постепенно реализуется установка инфраструктуры СОРМ, которая позволяет комплексно обрабатывать и хранить всю информацию из социальных сетей, мессенджеров, телефонных разговоров. В 2014-2015 годах в СОРМ стали интегрировать технологии глубокой инспекции пакетов (DPI).

В 2025 году параллельно с блокировкой популярных мессенджеров и соцсетей со стороны государственных органов началось навязывание использования прогосударственного мессенджера “Max”.

Таджикистан

Концепции и нормативное правовое регулирование

Основным концептуальным документом является Стратегия развития искусственного интеллекта до 2040 года. Таджикистан стал первой страной в Центральной Азии, принявшей национальную стратегию в сфере ИИ. Стратегия определяет ключевые направления интеграции ИИ в разные сферы жизни общества, а также ставит в качестве одной из целей разработку системы нормативного правового регулированию, включающую разработку специального законодательства и обновления существующего.

В целях реализации Стратегии при Агентстве по инновациям и цифровым технологиям при Президенте Республики Таджикистан создана Межведомственная комиссия по регулированию в сфере ИИ.

В 2025 году по инициативе Таджикистана Генеральная Ассамблея ООН единогласно приняла резолюцию "Роль искусственного интеллекта в создании новых возможностей для устойчивого развития в Центральной Азии", которая предусматривает создание Регионального центра ИИ в Душанбе.

Финансирование и стратегические проекты

В октябре 2025 года в Душанбе состоялась конференция AI Conf 2025 с участием более 20 стран. В рамках конференции были анонсированы ряд проектов:

- создание специализированной зоны в сфере ИИ Area AI Zone, членами которой станут местные стартапы и международные компании;

- запущен проект Soro в сотрудничестве UNICEF и стартапом zypl.ai по интеграции систем ИИ в сферу образования;
- анонсирована SoroLLM – модель ИИ, созданная на основе наборов данных на таджикском языке;
- объявлено, что компания darya.ai_ и индийская Yotta Data Services подписали соглашение о сотрудничестве для создания экологичного центра обработки данных для систем ИИ.

Помимо этого, государственные органы заключены соглашения о сотрудничестве с Huawei, Perplexity AI, Google DeepMind, NVIDIA, и Presight, Scale AI. Кроме того, в государственные органы и банки активно внедряется zypl.ai – один из ключевых страртапов страны в сфере кредитного скоринга.

Применение систем ИИ для цензуры

С конца 2015 года в стране в качестве основного элемента контроля трафика служит Единый центр коммутации электронных коммуникаций (ЕКЦ), созданный постановлением правительства. Этот документ обязывает всех операторов связи и интернет-провайдеров маршрутизировать весь международный трафик через государственный шлюз, управляемый Tojiktelecom. Несмотря на то, что в 2023 отдельные операторы получили возможность_напрямую закупить международный трафик, в 2025 году на базе Tojiktelecom был запущен единый национальный интернет-обменный узел (TJ-IX).

Полномочия органов по блокировке контента и интернет ресурсов прямо не прописаны в законе, однако проистекают из общих требований законов “Об информации”, “О СМИ”, “Правилах предоставления интернет услуг”. Органы власти в административном порядке блокируют ресурсы, публично черный список не размещен. Известно, что заблокированы Asia-Plus, Radio Ozodi (Радио Свобода).

Законы “О противодействии терроризму”, “О противодействии экстремизму”, “О чрезвычайном положении” также используются в

качестве оснований для ограничения доступа к интернету. Например, после силового воздействия на протесты в Горно-Бадахшанской автономной области действовало полное отключение интернета на 4 месяца.

В 2018 году парламент криминализирован использование функций “лайк” и “репост” в социальных сетях в отношении контента, связанного с терроризмом и экстремизмом, с максимальным наказанием до 15 лет лишения свободы (статья 179(3) УК). В мае 2025 года вступил в силу закон, отменяющий уголовную ответственность за “лайки”, однако к этому моменту по данной статье было осуждено более 1500 человек.

Несмотря на то что прямые свидетельства о применении систем ИИ для контроля за интернет-пространством отсутствуют, наличие законодательной базы делает данный вопрос сугубо техническим.

Применение систем ИИ для гласного и негласного наблюдения

Использование систем видеонаблюдения и биометрической идентификации технологий осуществляется в отсутствие специального нормативного правового регулирования. Правовую основу составляет Закон “Об оперативно-розыскной деятельности”. Система городского видеонаблюдения развивается в рамках проекта “Безопасный город” с 2013 года с постепенной установкой большего числа камера в крупных населенных пунктах. Стратегия развития ИИ также предусматривает возможность интеграции видеонаблюдения с интеллектуальными аналитическими системами, включая автоматизированный анализ транспортных и городских потоков. По открытым данным, устанавливается оборудование китайских производителей (Huawei).

С 2001 года операторам связи необходимо устанавливать технические средства СОРМ. По данным на 2023 год, в стране функционируют системы СОРМ-1 (телефония) и СОРМ-2 (интернет).

В ноябре 2025 года Tojiktelecom запустило национальный мессенджер Oriz с серверами, расположенными исключительно на территории страны. По свой сути он напоминает российский мессенджер MAX и казахстанский Aitu.

Узбекистан

Концепции и нормативное правовое регулирование

Основополагающим концептуальным документом является Стратегия развития технологий искусственного интеллекта до 2030 года. Стратегия предполагает широкое внедрение систем ИИ во все сферы деятельности общества и государства и разработку комплексного нормативного правового регулирования. Реализация разделена на три этапа: создание инфраструктуры (2024-2025), масштабирование (2026-2028) и коммерциализация (2028-2030).

В ноябре 2025 года Сенат одобрил проект закона, который вносит изменения в ряд нормативных, связанных с регулированием отношений, возникающих при применении систем ИИ.[4]

Важным элементом регулирования является также и требование о локализации данных на территории Узбекистана, установленное ст. 27[1] Закона "О персональных данных".

В декабре 2024 года был опубликован проект этических правил для разработки и применения систем ИИ.

Финансирование и стратегические проекты

Инфраструктура для развития цифровых инноваций в стране первоначально начала создаваться с 2019 года в рамках проекта IT Park Uzbekistan.

---

[4] На момент проведения исследования документ не был опубликован, однако на основе пресс-релизов можно сделать вывод, что он будет направлен на определение терминологии, установление правил для использования отдельных систем ИИ, а также уточнению особенностей обработки персональных данных.

Стратегия предусматривает выделение с 1 января 2025 года Министерству цифровых технологий беспроцентного кредита в размере 50 млн. долларов сроком на 5 лет, включая льготный период 2 года, для развития технологий ИИ.

Дополнительно указом президента выделено в 2026-2027 годах 100 млн. долларов для финансирования проектов, в том числе стартапов в социальной сфере и отраслях экономики, связанных с ИИ.

В 2025 году было объявлено о начале реализации нового инфраструктурного проекта в партнерстве с саудовской компанией DataVolt.Речь о строительстве дата-центров общей мощностью до 500 МВт и стоимостью 5 млрд. долларов к 2030 году.

Применение систем ИИ для цензуры

Центр мониторинга информационного пространства Узкомназората при взаимодействии с другими органами осуществляет поиск и обеспечивает удаление противоправной информации во внесудебном порядке. Единый реестр не находится в публичном доступе.

В судебном порядке блокировка экстремистских и террористических материалов осуществляется на основании решений судов общей юрисдикции, принимаемых по представлению уполномоченных правоохранительных органов. Списки материалов, признанных экстремистскими/террористическими, регулярно публикуются на сайте Верховного суда и в СМИ. Последняя версия списка насчитывает более 1600 ресурсов.

Внутренняя деятельность органов власти непрозрачна, поэтому невозможно с достаточной степенью уверенности сделать вывод о том, применяются ли системы ИИ государственными органами при поиске противоправного контента.

Прецедент полного отключения интернета имел место в июне-июле 2022 года в Каракалпакстане во время протестов против ограничения региональной автономии.

Применение систем ИИ для гласного и негласного наблюдения

В апреле 2019 года Huawei заключила контракт на 1 млрд. долларов на развертывание системы Safe City с 883 камерами в Ташкенте.

В рамках государственной программы по цифровизации и внедрению ИИ принято решение о пилотном внедрении системы распознавания лиц UzFace. Согласно постановлению Кабинета министров, проект планируется к запуску на входах в железнодорожные вокзалы Ташкента в 2025 – 2026 гг. как часть приоритетных инициатив по развитию ИИ. Ранее государственные структуры также рассматривали расширенное применение биометрических технологий, включая распознавание лиц и отпечатков пальцев, для нужд правоохранительных органов, а технология Face-ID включена в государственные сервисы идентификации через Mobile-ID.

С 2006 года все операторы связи в соответствии со ст. 18 Закона “О телекоммуникациях” обязаны установить СОРМ-совместимое оборудование.

Выводы

1. Государства региона демонстрируют существенную неоднородность в подходах к нормативному регулированию сферы ИИ. По степени развития специального законодательства можно выделить три группы:

- *Страны с комплексным подходом к регулированию*: Казахстан принял специальный Закон “Об искусственном интеллекте” (2025), Кыргызстан интегрировал главу о системах ИИ в Цифровой кодекс (2026). Несмотря на схожесть отдельных элементов регулирования с Регламентом ЕС по ИИ, данные законы представляют собой скорее отправную точку для регулирования, которое вынесено на уровень подзаконных актов. Это вызывает неопределенность с точки зрения защиты прав человека и существенные риски для защиты фундаментальных прав, в том числе права на тайну частной жизни и свободу информации.
- *Страны с концептуальным подходом к регулированию*: Россия, Узбекистан, Таджикистан и Азербайджан приняли стратегические документы и концепции развития ИИ, однако комплексное законодательство находится на этапе разработки. Характерной чертой является использование инструментов “мягкого права” (кодексы этики, добровольные стандарты), которые создают видимость регуляторной активности при фактическом отсутствии обязывающих норм.
- *Страны с несформированным подходом к регулированию*: Армения, Грузия и Беларусь не имеют ни специального законодательства, ни детализированных концептуальных документов в сфере ИИ. К ней применяются нормы общего законодательства.

2. В государствах с авторитарными признаками развитие нормативного регулирования ИИ направлено преимущественно на легитимацию применения технологий наблюдения, а не на защиту прав человека. Запреты отдельных ИИ-практик (манипулятивные методы, дискриминационная классификация) и ограничения по

степени риска, формально включенные в законодательство Казахстана и Кыргызстана, не распространяются на деятельность правоохранительных органов или содержат исключения для целей обеспечения национальной безопасности.

Одновременно законодательство о противодействии экстремизму и терроризму во всех исследованных странах содержит широкие и размытые формулировки, допускающие произвольное толкование и создающие правовую основу для ограничения свободы выражения мнений и права на неприкосновенность частной жизни в том числе с применением на государственном уровне систем ИИ, позволяющих автоматизировать процесс принятия решений.

3. Китай и Россия активно экспортируют репрессивные технологии в страны Евразии. Оборудование компаний Huawei, Hikvision и Dahua установлено во всех исследованных государствах. Проекты “Безопасный город” и “Умный город” в Казахстане, Узбекистане, Таджикистане, Кыргызстане и частично в других странах реализованы с использованием китайских технологий.

Российская инфраструктура СОРМ в разное время была внедрена во всех исследованных государствах за исключением Грузии. Система обеспечивает возможность перехвата телефонных переговоров и интернет-трафика без эффективного судебного контроля.

Диверсификация партнеров характерна для Армении (переориентация на США и Индию), Таджикистана (сотрудничество с Индией, ОАЭ, западными технологическими компаниями) и частично Казахстана (партнёрство с ОАЭ, Сингапуром). Однако эта диверсификация касается преимущественно вычислительной инфраструктуры и разработки языковых моделей, тогда как системы наблюдения остаются в значительной мере зависимыми от китайских и российских технологий.

4. Все исследованные государства располагают правовыми и техническими возможностями для ограничения доступа к интернет-контенту. Условно можно выделить следующие модели:

- *Централизованная модель с применением систем ИИ (Россия)*: функционирует развитая экосистема автоматизированных

решений (“Ревизор”, “Окулус”, “Вепрь”, “Мир”, АС “Мавр” и д.р.), обеспечивающая выявление и блокировку контента в режиме реального времени. Установка ТСПУ с функциями глубокой инспекции пакетов (DPI) позволяет осуществлять блокировки на уровне протоколов.

- *Централизованная модель с начальным или недоказанным уровнем применения систем ИИ (Азербайджан, Беларусь, Кыргызстан, Таджикистан)*: весь международный трафик маршрутизируется через государственные узлы, что обеспечивает возможность полного отключения интернета. Применение систем ИИ документально не подтверждено, однако масштаб блокировок (более 18 тыс. ресурсов в Беларуси) предполагает использование автоматизированных средств, в том числе на базе ИИ-технологий.

- *Децентрализованная модель (Армения, Грузия)*: блокировки носят точечный характер и осуществляются преимущественно в отношении контента, нарушающего законодательство (азартные игры, порнография, нарушения авторских прав). Вместе с тем в Грузии отмечается расширение оснований для блокировок (законы о “пропаганде ЛГБТ+”, об иностранных агентах).

5. Системы биометрической идентификации с использованием технологий распознавания лиц внедрены или внедряются во всех исследованных государствах. Наиболее развитые системы функционируют в России (более 1 млн камер, Единая биометрическая система и совокупность разных систем ИИ от нескольких производителей), Беларуси (платформа Kipod, более 60 тыс. камер) и Казахстане (более 1,6 млн камер, из которых 20,5 тыс. интегрированы с системами ИИ).

Характерной тенденцией является легализация биометрической идентификации постфактум: сначала технологии внедряются, затем принимается законодательство, легитимирующее их применение. При этом оно, как правило, не содержит процессуальных гарантий, механизмов независимого надзора и иных способов обеспечения прозрачности для общества.

6. Разработка “суверенных” моделей ИИ, позиционируемых как инструмент технологической независимости, создает беспрецедентные риски для прав человека.

Россия открыто декларирует курс на создание моделей, соответствующих “традиционным ценностям” и интересам государства. Модели YandexGPT и GigaChat функционируют со встроенными ограничениями на генерацию контента, противоречащего государственной политике. Аналогичные тенденции прослеживаются в Казахстане (KazLLM, AlemLLM), Кыргызстане (Акылай) и Таджикистане (SoroLLM).

Распространение “суверенных” модели ИИ порождает несколько групп рисков:

- Модели, обученные на контролируемых наборах данных, способны систематически искажать информацию по политически чувствительным темам, формируя альтернативную информационную реальность, воспринимаемую пользователем как объективную.
  Россия демонстрирует передовые практики применения современных ИИ-моделей для дезинформации: бот-фермы на базе ИИ, массовое генерирование дипфейков, целенаправленное “загрязнение” обучающих наборов данных для иностранных моделей ИИ (ChatGPT, Claude, Gemini и д.р.) пропагандистскими материалами.
- Интеграция передовых моделей ИИ вместе с системами мониторинга создает возможность автоматизированного выявления контента, ранее требовавшего активного человеческого участия. Это радикально расширяет охват цензуры. Сочетание передовых моделей ИИ с централизованным сбором данных о гражданах позволят персонализировать пропаганду и открыть возможности для превентивного выявления “неблагонадежных” лиц.
- Доступность открытых моделей ИИ (Llama, DeepSeek и д.р.), которые могут быть дообучены без ограничений со стороны разработчиков. позволит создавать адаптированные модели

с минимальными ресурсами для последующей интеграции в репрессивную инфраструктуру авторитарных стран.

Дмитрий Кутейников и Сергей Кузнецов для RKS Global

RKS Global