

Регулирование видеонаблюдения по регионам - трансграничный справочник

Как правила наблюдения и биометрии различаются по регионам и как один продукт соответствует всем сразу. Инженерное руководство, не юр. совет - уточняйте конкретику у юриста.

Три вопроса делят любой режим

1) Является ли обычное видео опознаваемого человека уже ПЕРСОНАЛЬНЫМИ ДАННЫМИ (тогда весь закон действует до любой аналитики)? 2) Является ли ШАБЛОН ЛИЦА более высокой 'биометрической / особой' категорией со своим барьером согласия? 3) ПУБЛИЧНОЕ или ЧАСТНОЕ пространство - и кто наблюдает: частный оператор или госорган? Ответы, а не репутация страны, решают строгость регулирования. Барьер биометрии и модель принуждения - там, где трансграничные продукты чаще всего проходят или падают.

Матрица регионов (ПД = персональные данные; актуально на середину 2026)

Регион / закон	Видео = ПД?	Барьер биометрии	Принуждение
EU - GDPR + AI Act	Да	Особая категория (ст. 9); живое распознавание в публице под запретом	Регуляторы; штраф до 4% оборота
UK - UK GDPR + DPA 2018	Да	Особая категория	ICO + отд. кодекс камер
US - Illinois (BIPA)	Через закон штата	Письменное согласие до захвата	Иск от частных лиц + ущерб
US - большинство штатов (~20)	Чувств. данные	'Чувств. данные' - opt-in / opt-out	Генпрокурор штата
Canada / Quebec	Да	Согласие; Quebec: уведомить CAI до БД	OPC / CAI
Brazil - LGPD	Да	Чувствительные персональные данные	ANPD
China - PIPL + FR Measures	Да	Согласие + ЛОКАЛЬНОЕ хранение	CAC/MPS; учёт > 100k
India - DPDP Act 2023	Да (поэтапно)	Нет отдельной категории биометрии	Совет по защите данных
Australia - Privacy Act 1988	Да	'Чувствительная информация' - согласие	OAIC + новый деликт

Ловушка охвата

Закон следует за ВАШИМИ СУБЪЕКТАМИ, а не за офисом. GDPR ст. 3 достаёт компанию без присутствия в ЕС, если она предлагает услуги или отслеживает поведение людей в ЕС - а аналитика камер это отслеживание. У PIPL Китая и LGPD Бразилии похожие экстерриториальные крючки. Считайте обязанности по тому, где снимают людей.

Резидентность данных

Где лежат байты - это архитектура, а не только бумаги. ЕС ограничивает вывоз персональных данных из ЕЕА без механизма передачи (adequacy / SCC). Китай по умолчанию хранит данные лица ЛОКАЛЬНО. В США общего правила нет. Держите запись и шаблоны региона в регионе; через границу - только обезличенные метаданные.

Базовая линия strictest-wins - соберите её один раз

[] Явное opt-in согласие ДО любого захвата биометрии (EU, Illinois, Quebec, China). [] Проведите DPIA / оценку воздействия до запуска (EU, Quebec; ожидается и в других). [] Минимизируйте данные - предпочитайте аналитику на устройстве или только счётчики, чтобы не хранить опознающее видео. [] Чёткое уведомление и таблички у каждой камеры. [] Ограничьте хранение кратчайшим обоснованным сроком. [] Храните данные региона там, где требует строжайший регион (локальное хранение в Китае - вынуждающий случай). [] Берите строжайшее правило по КАЖДОЙ оси - согласие, резидентность, хранение, иски - а не один регион целиком.

Это инженерное руководство, не юридический совет. GDPR Reg. (EU) 2016/679 (ст. 3/9/35); EDPB Guidelines 3/2019; EU AI Act (ст. 5; high-risk Annex III перенесён на 2 дек 2027 по Digital Omnibus от 7 мая 2026, ожидается принятия); Illinois BIPA 740 ILCS 14; Texas CUBI; Washington RCW 19.375; China FR Measures (CAC/MPS, 1 июн 2025) + PIPL; India DPDP Act 2023 + Rules 2025; Australia Privacy Act 1988; Canada PIPEDA + Quebec Law 25; Brazil LGPD даны для планирования - уточняйте конкретику ваших юрисдикций у юриста.