Surveillance Regulation by Region - Cross-Border Quick Reference

How surveillance and biometric rules differ across regions, and how one product complies with all of them. Engineering guidance, not legal advice - confirm specifics with qualified counsel.

Three questions split every regime

1) Is plain video of an identifiable person already PERSONAL DATA (so the whole privacy law applies before any analytics)? 2) Is a FACE TEMPLATE a higher 'biometric / special' category with its own consent gate? 3) PUBLIC or PRIVATE space - and is the watcher a private operator or a public authority? The answers, not a country's reputation, decide how heavily a deployment is regulated. The biometric gate and the enforcement model are where most cross-border products succeed or fail.

The regional matrix (PD = personal data; current to mid-2026)

Region / law	Video = PD?	Biometric gate	Enforcement
EU - GDPR + AI Act	Yes	Special category (Art. 9); public live face matching banned	Regulators; fines to 4% turnover
UK - UK GDPR + DPA 2018	Yes	Special category	ICO + separate camera code
US - Illinois (BIPA)	Via state law	Written consent before capture	Private right of action + damages
US - most states (~20)	Sensitive-data	'Sensitive data' - opt-in / opt-out	Attorney general
Canada / Quebec	Yes	Consent; Quebec: notify CAI before DB	OPC / CAI
Brazil - LGPD	Yes	Sensitive personal data	ANPD
China - PIPL + FR Measures	Yes	Separate consent + LOCAL storage	CAC/MPS; register > 100k
India - DPDP Act 2023	Yes (phase-in)	No separate biometric category	Data Protection Board
Australia - Privacy Act 1988	Yes	'Sensitive information' - consent	OAIC + new statutory tort

The reach trap

The law follows your SUBJECTS, not your office. GDPR Art. 3 reaches a company with no EU presence that offers services to, or monitors the behaviour of, people in the EU - and camera analytics is monitoring. China's PIPL and Brazil's LGPD carry similar extraterritorial hooks. Map obligations by where people are filmed.

Data residency

Where bytes may sit shapes architecture, not just paperwork. The EU restricts moving personal data outside the EEA without a transfer mechanism (adequacy / SCCs). China defaults facial data to LOCAL storage. The US has no general rule. Keep each region's footage and templates in-region; move only minimised metadata across borders.

The strictest-wins baseline - build this once

[ ] Explicit, opt-in consent BEFORE any biometric capture (EU, Illinois, Quebec, China). [ ] Run a DPIA / privacy impact assessment before launch (EU, Quebec; expected elsewhere). [ ] Minimise data - prefer on-device or count-only analytics so identifying footage is not retained by default. [ ] Clear notice and signage at every camera. [ ] Cap retention to the shortest defensible window. [ ] Store each region's data where the strictest region requires (China local storage is the forcing case). [ ] Take the hardest rule on EACH axis - consent, residency, retention, enforcement - not one region wholesale.

This is engineering guidance, not legal advice. GDPR Reg. (EU) 2016/679 (Art. 3/9/35); EDPB Guidelines 3/2019; EU AI Act (Art. 5; Annex III high-risk deferred to 2 Dec 2027 per the 7 May 2026 Digital Omnibus, pending adoption); Illinois BIPA 740 ILCS 14; Texas CUBI; Washington RCW 19.375; China FR Measures (CAC/MPS, 1 Jun 2025) + PIPL; India DPDP Act 2023 + Rules 2025; Australia Privacy Act 1988; Canada PIPEDA + Quebec Law 25; Brazil LGPD are summarised for planning - confirm specifics for your jurisdictions with qualified counsel.