The Video-Analytics Catalogue - One-Page Reference

What a surveillance system can detect: the seven analytics families, where each runs, how each surfaces into the VMS, and the honest accuracy of each. Representative 2026 figures.

A. The seven analytics families (what each detects)

- Object detection + classification: people, vehicles, objects, and what they are - the foundation, runs on the camera (edge).
- Tracking + re-identification: one object across frames and cameras (a movement trail, not an identity) - edge to server.
- Face recognition: a specific identity from a face template - biometric, runs on a server/cloud (see Section C).
- License-plate recognition (LPR/ANPR): a plate read as text - personal data, a plate camera plus server (see Section C).
- Behavioral rules: line-crossing, zone intrusion, loitering, crowd, left/removed object - you author the rule in the VMS.
- Anomaly detection: departures from a learned normal, where you cannot enumerate every bad event - server/cloud.
- Search by event: query months of footage by what was detected - the payoff; reads the metadata the others produced.

B. Accuracy is a range, never 100%

- Object detection: ~38-55% mAP@50-95 on the strict COCO measure; higher operational precision/recall in a fixed scene.
- LPR: ~90-98% in good conditions, can exceed 99% in a controlled lane, falls below ~70-80% with motion, dirt, angle, weather.
- Face recognition: near-perfect in controlled NIST tests (~0.07% miss), worse on wide-angle/low-light video, varies by demographic.
- Judge by false-alarm volume: a '99% accurate' detector on 100,000 daily candidates still yields ~1,000 false alarms a day.

C. Two analytics are a legal gate, not a feature

- Face recognition and LPR process biometric or personal data - a privacy review comes before any technical work.
- EU: GDPR Art. 9 (special-category biometric data) + the EU AI Act (real-time public-space biometric ID banned for law enforcement since Feb 2025; high-risk biometric duties from 2 Dec 2027).
- US: Illinois BIPA (740 ILCS 14) - private right of action, $1,000 negligent / $5,000 intentional; SB 2979 (2024) limits to a single recovery.
- Keep biometric processing on hardware you control under a lawful basis; the full law is the Privacy & Compliance block.

D. How to choose

- Pick the analytics the job needs - not every box on the vendor feature list.
- Demand precision AND recall in your lighting and camera placement, never a single '99%'.
- Place the two biometric analytics behind a privacy/legal review before scoping the build.

How analytics surface into the VMS: increasingly via ONVIF Profile M, the standard for analytics metadata and events (object classification; metadata for vehicle, plate, face, body; events for counting, LPR, and face recognition) - a conformant analytic can be a camera, a server, or a cloud service. Where analytics run (edge vs cloud) is a separate decision that sets latency, bandwidth, and privacy. Engineering guidance, not legal advice; confirm specifics with qualified counsel. Figures are representative for 2026 and move with scene, lighting, angle, and tuning. Sources: ONVIF Profile M; GDPR Reg. (EU) 2016/679 Art. 9; EU AI Act Reg. (EU) 2024/1689; Illinois BIPA 740 ILCS 14; EDPB Guidelines 05/2022; NIST FRTE/FRVT; COCO/Ultralytics; ANPR survey literature.