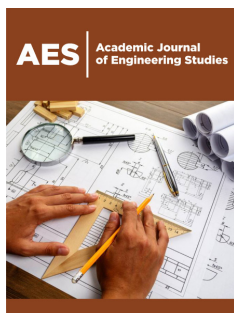


From Watching People to Understanding Situations: Balancing Public Safety, Privacy and Social Acceptance in AI Video Surveillance

ISSN: 2694-4421

**Rafael Rodrigo-Guillen***

Associate Professor, Department of Computer Science and Technology, University of Alicante, Spain

Abstract

Artificial intelligence enabled video surveillance can improve public safety by detecting crowd gatherings, abnormal behaviour and emerging hazards, but it also intensifies concerns about privacy and social acceptance. This Opinion argues that the central design question should not be how much information can be extracted from video, but how little personal information is actually required to achieve a legitimate safety objective. Situation-oriented systems based on counting, density, flow and temporal anomaly detection may preserve useful security capabilities while reducing unnecessary identification, retention and profiling. Privacy by design can therefore be treated not as a barrier to intelligent surveillance, but as an engineering requirement.

Keywords: Artificial intelligence; Video surveillance; Public safety; Privacy; Anomaly detection; Social acceptance

***Corresponding authors:** Rafael Rodrigo-Guillen, Associate Professor, Department of Computer Science and Technology, University of Alicante, Spain

Submission: 📅 October 13, 2026

Published: 📅 October 27, 2026

Volume 4 - Issue 3

How to cite this article: Rafael Rodrigo-Guillen*. The UAE's Scorching Heat is the New Normal. Academic J Eng Stud. 4(3). AES.000588. 2026.
DOI: [10.31031/AES.2026.04.000588](https://doi.org/10.31031/AES.2026.04.000588)

Copyright@ Rafael Rodrigo-Guillen, This article is distributed under the terms of the Creative Commons Attribution 4.0 International License, which permits unrestricted use and redistribution provided that the original author and source are credited.

Introduction

Video surveillance is an established component of public-safety strategies in cities, transport infrastructures and mass gatherings. Artificial intelligence (and computer vision) are now transforming cameras from passive recording devices into systems able to detect people, estimate crowd density and identify abnormal situations. Our recent review showed the growing role of deep learning in detecting gatherings and anomalous events in public spaces [1]. This progress raises a question that is technological, legal and social at the same time: does improving public safety require collecting increasingly detailed information about the individuals being protected?

From surveillance to situation awareness

The security value of video surveillance should not be dismissed. A major meta-analysis found Closed-Circuit Television (CCTV) to be associated with a significant but modest reduction in crime overall, with effects varying across settings [2]. Intelligent analysis also extends surveillance beyond crime prevention: unusual crowd growth, congestion, panic movements or sudden changes in pedestrian flow may precede hazardous events. Yet many of these tasks do not require knowing who a person is. Detecting that occupancy is rising abnormally or that a crowd is deviating from its expected temporal pattern can be achieved from aggregated variables such as counts, density or flow. This suggests a useful distinction between surveillance centered on people and surveillance centered on situations.

That distinction is operationally important. A system intended to detect overcrowding at a station entrance has a different informational need from a system intended to identify a suspect

after a serious offence. Conflating these purposes encourages unnecessary data collection. For preventive surveillance, useful information may lie primarily in the temporal dynamics of the monitored environment rather than in the identity of particular individuals, for instance, changes in occupancy, sudden increases in density, unexpected shifts in pedestrian flow, or significant departures from established behavioral patterns. Designing around those variables can preserve the early-warning function of surveillance while avoiding an assumption that persistent identity is always technically necessary.

Privacy and social acceptance

Public acceptance cannot be assumed simply because surveillance is presented as a security measure. A systematic review of 50 studies found that acceptance of public-space surveillance depends on the technology used, its location, perceived effectiveness, privacy concerns, trust and institutional legitimacy [3]. Research across nine European Union countries likewise shows that citizens do not make a simple privacy-for-security trade-off. Trust in the organization operating the system is crucial [4]. European data-protection law provides a compatible engineering principle. Where the General Data Protection Regulation (GDPR) applies, it requires data minimization [5], while guidelines from the European Data Protection Board emphasize necessity and proportionality in video surveillance [6]. Police processing for criminal-law-enforcement purposes is governed by a separate regime. In Spain, Organic Law 7/2021 specifically regulates police video surveillance and requires proportionality. For fixed cameras in public places, it expressly requires assessment of suitability and minimum intervention [7]. Under the EU Artificial Intelligence Act, law-enforcement use of systems that identify individuals biometrically from a distance and in real time in public areas is confined to narrowly specified circumstances and stringent safeguards [8].

Social acceptance is therefore partly a governance problem, not merely a communication problem. Notices stating that an area is under video surveillance provide limited reassurance if citizens do not know whether images are being retained, whether facial or biometric analysis is performed, or whether data collected for crowd safety may later be reused for unrelated purposes. Transparency should describe the actual processing chain in terms that non-specialists can understand. Equally important is purpose discipline: a system introduced to estimate crowd risk should not gradually become an identification or profiling infrastructure simply because additional analytical functions become technically available. Preventing this form of function creep is central to preserving both proportionality and institutional trust.

Security without identification

These principles invite a different design question: not how much information can be extracted from a video stream, but what is the minimum information required for the safety objective. A privacy-oriented pipeline could progressively abstract information as follows: video image, person detection, aggregated crowd information, temporal behavior and anomaly alert. Images may be

processed locally, converted as early as possible into non-identifying or aggregated representations, and discarded when retention is unnecessary. This does not mean that the whole processing chain automatically falls outside data-protection law, because identifiable images may still be processed at an earlier stage. However, edge processing, short retention, irreversible aggregation where feasible and avoidance of unnecessary biometric identification can substantially reduce privacy exposure. Recent work on privacy-preserving video anomaly detection shows that anomaly-detection performance and protection of personally identifiable information are increasingly being addressed jointly [9].

A practical implementation should make these safeguards architectural rather than optional. Whenever technically feasible, raw frames can remain at the edge device, while only derived variables or alerts leave the local processing environment. Retention periods can be tied to a defined operational purpose instead of being determined by available storage capacity. Aggregation should also be designed carefully: feature vectors, trajectories or persistent identifiers may still permit individuals to be distinguished even when names or faces have been removed. Consequently, privacy preservation cannot be reduced to deleting facial images. It requires examining what information remains linkable across time and whether that link ability is necessary for the task.

There is also an important performance dimension. A privacy-preserving system should not be judged only by whether it conceals identity, just as a surveillance system should not be judged only by detection accuracy. For public-safety applications, useful evaluation should consider detection delay, false alarms, robustness to changing crowd conditions and the amount of personal information processed to obtain that performance. This creates a more meaningful engineering objective: achieve the required level of situational awareness with the lowest reasonable privacy cost. Human oversight remains essential, because an anomaly score is an indication that conditions differ from expectation, not proof that a dangerous or unlawful event is occurring.

Accountability should also be designed into the system. An operator claiming that a surveillance architecture is privacy-preserving should be able to specify which data enters the model, which representations are retained, who can access them, how long they persist and under what conditions an alert leads to review of the original video. These choices should be auditable and revisited when the purpose or technical capabilities of the system change. This is especially relevant because modern models can derive rich representations that are not visually recognizable as personal information yet may still distinguish or link individuals over time. Privacy by design is therefore not a one-time anonymization step, but a lifecycle requirement extending from acquisition and inference to storage, access, escalation and deletion. Framing privacy in these operational terms also improves public accountability: citizens can evaluate concrete safeguards rather than being asked to trust a generic promise that surveillance is used only for safety.

The appropriate level of abstraction will also depend on context. A stadium exit, an airport security zone and a pedestrian

square present different risks, response times and legal bases, so a single surveillance architecture should not be treated as universally optimal. In some environments, anonymous counts may be sufficient. In others, short-lived trajectories or temporary access to original frames may be justified for verification. The design principle should remain the same: begin with the least intrusive representation capable of meeting the defined safety need, and introduce more identifying information only when a specific, documented purpose requires it. This reverses the usual tendency to collect everything first and decide later what is useful.

A further practical implication concerns procurement and evaluation. Public bodies should not compare intelligent surveillance systems only with headline detection accuracy. Technical specifications can also define which data categories may be processed, whether biometric functions are disabled by default, where raw images are handled, how long derived information is retained, which events permit access to original footage and what audit trail is generated. These requirements make privacy measurable rather than aspirational. Operational evaluation should likewise report false alarms and the burden placed on human operators, because a system that generates excessive alerts may undermine trust or encourage broader monitoring to compensate. Security effectiveness, privacy exposure and human oversight should therefore be assessed together throughout deployment, rather than treating data protection as a final compliance check after the technical architecture has already been fixed.

Conclusion

The traditional debate between surveillance and privacy is often framed as a zero-sum choice. AI could intensify that conflict if its purpose is to identify, classify and retain as much information as possible about every person observed. It could also provide part of the solution if systems are designed around purpose limitation, data minimization and situation-oriented anomaly detection. This argument does not imply that identification is never justified. There are circumstances in which lawful identification may be necessary for a specific investigative or security purpose. The key point is that identification should not become the default technical architecture for tasks that can be accomplished without it. Public authorities should therefore explain not only where cameras are installed, but

what algorithms extract, what is discarded, how long information is retained and whether identification is performed. Public safety should not require knowing who people are when knowing what is happening is enough. The most advanced surveillance system may be the one that detects what matters while learning the least possible about the individuals being protected.

Acknowledgement

No external funding was received for this work.

Conflict of Interest

The author declares no conflict of interest.

References

1. Rodrigo-Guillen R, Garcia-D'Urso N, Mora-Mora H, Azorin-Lopez J (2025) Detecting abnormal behavior events and gatherings in public spaces using deep learning: A review. *Journal of Sensor and Actuator Networks* 14(4): 69.
2. Piza EL, Welsh BC, Farrington DP, Thomas AL (2019) CCTV surveillance for crime prevention: A 40-year systematic review with meta-analysis. *Criminology & Public Policy* 18(1): 135-159.
3. Bates L, Bayerl PS, Akhgar B (2025) Which factors affect acceptance of public space surveillance? A systematic literature review. *Journal of Urban Technology* 32(3): 193-212.
4. Degli Esposti S, Ball K, Dibb S (2021) What's in it for us? Benevolence, national security, and digital surveillance. *Public Administration Review* 81(5): 862-873.
5. European Parliament and Council of the European Union (2016) Regulation (EU) 2016/679 (General Data Protection Regulation). *Official Journal of the European Union* L119: 1-88.
6. European Data Protection Board (2020) Guidelines 3/2019 on processing of personal data through video devices. Version 2.0, adopted 29 January 2020.
7. Spain (2021) Organic Law 7/2021, of May 26, on the protection of personal data processed for the purposes of prevention, detection, investigation and prosecution of criminal offenses and execution of criminal penalties. *Official State Gazette* 126.
8. European Parliament and Council of the European Union (2024) Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*.
9. Liu Y, Liu S, Zhu X, Yang H, Li J, et al. (2026) Privacy-preserving video anomaly detection: A survey. *IEEE Transactions on Neural Networks and Learning Systems* 37(1): 2-21.