

ARTICOLO DI RICERCA APPLICATA

Videosorveglianza e biometria nel retail della moda: cosa può fare un brand, e cosa no

Video surveillance and biometrics in fashion retail: what a brand can and cannot do

Maria Luisa Portaluppi

DPO, Lead Auditor ISO/IEC 27001 e ISO/IEC 42001 – Portaluppi Research & Innovation, Osservatorio GlamAura Hub

ABSTRACT

Dopo gli episodi di metà ottobre 2026 nel centro di Milano, molti punti vendita del Quadrilatero della Moda hanno rafforzato le misure di protezione fisica. La risposta successiva, tecnologica, è spesso l'estensione della videosorveglianza e, talvolta, l'interesse per sistemi capaci di riconoscere le persone. L'articolo ricostruisce il quadro normativo applicabile a un brand della moda in Italia: i requisiti del GDPR e delle Linee guida EDPB 3/2019 per la videosorveglianza tradizionale, i vincoli dell'art. 4 dello Statuto dei lavoratori, la moratoria nazionale sui sistemi di riconoscimento biometrico prorogata al 31 dicembre 2027 e le pratiche vietate dall'art. 5 del Regolamento (UE) 2024/1689 (AI Act). Ne deriva una checklist operativa di dieci controlli, pensata per il punto vendita, che distingue ciò che è lecito con le dovute cautele da ciò che oggi non è consentito.

ABSTRACT (ENGLISH)

Following the mid-October 2026 events in central Milan, many stores in the Fashion District strengthened their physical protection. The next, technological response is often the expansion of video surveillance and, at times, interest in systems able to recognise people. This paper reconstructs the legal framework applicable to a fashion brand in Italy: GDPR requirements and EDPB Guidelines 3/2019 for conventional video surveillance, the constraints of Article 4 of the Italian Workers' Statute, the national moratorium on biometric recognition systems extended to 31 December 2027, and the practices prohibited by Article 5 of Regulation (EU) 2024/1689 (AI Act). It derives a ten-point operational checklist for the store, separating what is lawful with appropriate safeguards from what is currently not permitted.

Parole chiave: videosorveglianza; GDPR; riconoscimento facciale; AI Act; retail; moda; DPIA; Statuto dei lavoratori.

Keywords: video surveillance; GDPR; facial recognition; AI Act; retail; fashion; DPIA; workplace monitoring.

1. Introduzione

Nelle notti successive agli scontri di metà ottobre 2026, nel Quadrilatero della Moda di Milano molte vetrine sono state coperte da pannelli. Chiudere le vetrine è la risposta immediata. Subito

dopo ne arriva un'altra: più telecamere, impianti più evoluti e, a volte, la tentazione di software che riconoscono le persone.

La sicurezza del punto vendita è un interesse legittimo. Ogni telecamera, però, tratta dati personali di clienti, passanti e dipendenti. Un impianto progettato male espone il brand a sanzioni e, soprattutto, incrina la fiducia dei clienti, che nel sistema moda è parte del valore del marchio. L'obiettivo di questo contributo è offrire ai brand un quadro sintetico e operativo di ciò che è consentito e di ciò che non lo è.

2. Metodo

Il lavoro è un'analisi documentale delle fonti normative e di indirizzo vigenti al 25 ottobre 2026: Regolamento (UE) 2016/679, Linee guida EDPB 3/2019 sul trattamento dei dati personali attraverso dispositivi video, indicazioni e FAQ del Garante per la protezione dei dati personali, art. 4 della L. 300/1970, normativa nazionale sulla moratoria dei sistemi di riconoscimento biometrico e Regolamento (UE) 2024/1689. Le indicazioni sono tradotte in controlli verificabili per il punto vendita.

3. La videosorveglianza tradizionale

Una telecamera in negozio è lecita se è necessaria alla sicurezza e alla tutela del patrimonio, se la finalità è documentata e se il trattamento rispetta i principi di minimizzazione e limitazione della conservazione.

Informativa di primo livello. Il cartello va collocato in posizione visibile prima dell'area ripresa. Indica il titolare, la finalità, i tempi di conservazione e rimanda all'informativa completa, anche tramite QR code.

Conservazione. Per finalità di sicurezza e tutela del patrimonio, le indicazioni del Garante e dell'EDPB orientano verso tempi brevi, nell'ordine di 24-72 ore, con cancellazione automatica. Periodi più lunghi richiedono una motivazione specifica, ad esempio una denuncia in corso.

Inquadrature. Ingressi, casse e magazzino possono essere ripresi; strade, marciapiedi e vetrine di terzi solo nello stretto indispensabile. Spogliatoi e servizi igienici sono esclusi.

Valutazione d'impatto (DPIA). È necessaria quando l'impianto sorveglia in modo sistematico un'area accessibile al pubblico su larga scala o impiega tecnologie innovative, come l'analisi automatica dei comportamenti. Va svolta prima dell'attivazione.

Lavoratori. Se l'impianto può riprendere il personale, l'art. 4 dello Statuto dei lavoratori richiede l'accordo con le rappresentanze sindacali o, in mancanza, l'autorizzazione dell'Ispettorato del lavoro. I dipendenti vanno informati.

Accessi e comunicazione delle immagini. Solo persone autorizzate e istruite, con credenziali personali e accessi tracciati. Le immagini si consegnano all'autorità giudiziaria o alle forze dell'ordine su richiesta; non si diffondono, né sui social né altrove.

Fornitori. L'installatore o il gestore dell'impianto e del cloud che tratta le immagini per conto del brand va nominato responsabile del trattamento ai sensi dell'art. 28 GDPR, con chiarezza su dove sono conservate le immagini.

4. Biometria e riconoscimento facciale

La tentazione più forte, dopo una notte di vetrine rotte, è la telecamera «intelligente» che riconosce i volti e segnala chi è già entrato in passato. In Italia, oggi, un punto vendita non può farlo.

La moratoria nazionale. La legge di conversione del decreto Milleproroghe, approvata a marzo 2026, ha esteso fino al 31 dicembre 2027 il divieto di installare e utilizzare impianti di videosorveglianza con sistemi di riconoscimento biometrico nei luoghi pubblici o aperti al pubblico, anche da parte di soggetti privati. Un negozio è un luogo aperto al pubblico.

L'AI Act. Dal 2 febbraio 2025 l'art. 5 del Regolamento (UE) 2024/1689 vieta, tra le altre pratiche, la creazione o l'ampliamento di banche dati di riconoscimento facciale mediante raccolta non mirata di immagini, il riconoscimento delle emozioni sul luogo di lavoro, la categorizzazione biometrica volta a dedurre caratteristiche sensibili e, per finalità di contrasto, l'identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico, salvo eccezioni tassative e autorizzate. I sistemi di identificazione biometrica remota non vietati rientrano tra i sistemi ad alto rischio.

La distinzione decisiva. Una telecamera che registra immagini, conservate per pochi giorni e consegnate alle autorità quando serve, è lecita nel rispetto delle regole del paragrafo 3. Un software che trasforma i volti dei clienti in dati biometrici per riconoscerli non lo è.

5. Checklist operativa per il punto vendita

CONTROLLO	COSA VERIFICARE
Finalità	Sicurezza e tutela del patrimonio, scritta e documentata
Cartello	Visibile prima dell'area ripresa, con rimando all'informativa completa
Inquadrature	Solo le aree necessarie; niente strada né terzi; mai spogliatoi e servizi
Conservazione	24–72 ore con cancellazione automatica; tempi più lunghi solo se motivati
DPIA	Svolta prima dell'attivazione, se l'area è aperta al pubblico su larga scala o il software analizza comportamenti
Lavoratori	Accordo sindacale o autorizzazione dell'Ispettorato; personale informato
Fornitore	Nomina a responsabile (art. 28 GDPR); luogo di conservazione delle immagini
Accessi	Persone autorizzate, credenziali personali, accessi registrati
Funzioni «intelligenti»	Riconoscimento facciale disattivato: vietato in Italia fino al 31 dicembre 2027
Registro	Trattamento inserito nel registro delle attività di trattamento

Tabella 1 – Dieci controlli prima di installare o ampliare un impianto di videosorveglianza in negozio.

6. Discussione e limiti

L'analisi si concentra sul quadro italiano ed europeo vigente alla data indicata. La moratoria nazionale ha scadenza fissata e il quadro dell'AI Act per i sistemi ad alto rischio è in fase di applicazione progressiva: entrambi andranno monitorati. Il contributo non esamina i trattamenti svolti dalle

forze dell'ordine né i casi di videosorveglianza urbana gestita dagli enti locali, che seguono regole proprie.

7. Conclusioni

Proteggere un negozio e rispettare i clienti non sono obiettivi in conflitto. Un impianto progettato bene è anche più utile alle indagini: immagini nitide, conservate per il tempo giusto, consegnate a chi deve usarle. Nel sistema moda, dove la relazione con il cliente è parte del valore del marchio, la sicurezza fatta bene è anche una forma di rispetto.

RIFERIMENTI

1. Regolamento (UE) 2016/679 (Regolamento generale sulla protezione dei dati), artt. 5, 13, 28, 30, 35.
2. Regolamento (UE) 2024/1689 (AI Act), art. 5 e Allegato III.
3. European Data Protection Board, Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video, versione 2.0, 29 gennaio 2020.
4. Legge 20 maggio 1970, n. 300 (Statuto dei lavoratori), art. 4.
5. Garante per la protezione dei dati personali, Videosorveglianza – indicazioni e FAQ: [garanteprivacy.it/videosorveglianza](https://www.garanteprivacy.it/videosorveglianza).
6. Hermes Center, Estensione della moratoria sul riconoscimento biometrico, comunicato del 12 marzo 2026.
7. Agenda Digitale, «Riconoscimento facciale nei luoghi pubblici: stop fino al 2027».
8. Cybersecurity360, «Privacy e videosorveglianza: ecco gli obblighi del titolare del trattamento».

Contributo a carattere informativo e di ricerca applicata; non sostituisce una consulenza legale sul caso specifico.
Fonti aggiornate al 25 ottobre 2026.