Uso dei Droni (UAS/APR) da parte delle Polizie Locali

Ricerca giuridica

Profili di legittimità, limiti, finalità, procedure operative e utilizzabilità probatoria

Ivrea, 1° marzo 2026 (ver. 1.0)
di Enrico Capirone

La questione della liceità dell'utilizzo di droni (UAS/APR) da parte delle Polizie locali presenta, allo stato dell'arte normativo e giurisprudenziale, una complessità articolata su più livelli: quello aeronautico (normativa EASA/ENAC), quello relativo alla pubblica sicurezza e alla sicurezza urbana (riparto di competenze tra Forze di polizia statali e polizie locali), quello della protezione dei dati personali (GDPR, D.Lgs. 51/2018) e quello della utilizzabilità probatoria delle immagini raccolte (c.p.p.).

In sintesi, le conclusioni dello studio che abbiamo condotto e vi proponiamo sono le seguenti:

- **Le Polizie locali** possono legittimamente **utilizzare droni per finalità prettamente amministrative** (accertamento abusi edilizi, rilevamento sinistri, monitoraggio ambientale in aree remote, protezione civile, controllo del territorio senza finalità di PS), nel rispetto della normativa aeronautica ENAC/EASA e degli obblighi GDPR (in primis la DPIA).
- **L'uso per finalità di pubblica sicurezza (PS)** è oggetto di **acceso dibattito interpretativo**. La posizione più restrittiva (Ministero dell'Interno/Garante Privacy) lo riserva alle Forze di polizia ex art. 16 L. 121/1981. La posizione contraria (ANVU) argomenta che il D.M. 13.06.2022 regola le "modalità" senza introdurre un divieto assoluto. In attesa di chiarimento legislativo, si raccomanda la massima cautela e l'acquisizione preventiva di titolo formale.
- **Per la "sicurezza urbana integrata"** (prevenzione criminalità diffusa/predatoria su pubblica via), il canale proprio è il Patto Prefetto-Sindaco ex D.L. 14/2017. Per le funzioni ausiliarie di pubblica sicurezza in senso stretto, il canale è invece la richiesta motivata dell'autorità competente con disposizione del Sindaco ex L. 65/1986. I due canali non sono fungibili: si applicano a finalità distinte e producono effetti giuridici diversi sulla catena di comando e sulla titolarità del trattamento dati. Il Garante Privacy ha ribadito che una delibera interna del Comune non è sufficiente a legittimare tale uso.
- **Le riprese video su luoghi pubblici** sono tendenzialmente utilizzabili come prova documentale ex art. 234 c.p.p.; ma la captazione dell'interno di abitazioni o spazi di vita privata configura il reato di cui all'art. 615-bis c.p. e rende le immagini inutilizzabili come prova.
- **In via di massima prudenza giuridica**, si raccomanda alle Polizie locali di: (a) ottenere Patto Prefetto-Sindaco o delega ex L. 65/1986 per ogni uso in finalità di sicurezza urbana/PS; (b) condurre sempre la DPIA; (c) adottare un regolamento interno; (d) predisporre la catena di custodia per l'uso probatorio; (e) notificare ANSV entro 60 min. in caso di incidente.

Licenza e diritti d'uso

Disclaimer

La presente ricerca ha finalità esclusivamente informativa e di supporto operativo.
I contenuti proposti non costituiscono consulenza legale, tecnica o amministrativa personalizzata e devono essere adattati, verificati e validati da ciascuna Amministrazione in funzione delle proprie specifiche esigenze, del contesto operativo, delle risorse disponibili e del quadro normativo applicabile al caso concreto.
iSimply S.r.l., i suoi autori e collaboratori declinano ogni responsabilità, diretta o indiretta, per eventuali danni, perdite, sanzioni o conseguenze derivanti dall'utilizzo dei contenuti della guida senza le necessarie verifiche, personalizzazioni e adeguamenti.
L'utilizzo delle informazioni contenute nel documento avviene sotto la piena responsabilità dell'Ente utilizzatore.
È raccomandato che ogni Piano redatto sulla base del presente modello sia sottoposto a verifica da parte di soggetti qualificati e approvato formalmente dalle autorità competenti all'interno dell'Ente.

Sommario

Nota metodologica

Il presente documento è destinato ai Comandanti di Polizia Locale e ai loro consulenti legali. È concepito come strumento operativo difendibile in sede di interlocuzione con Prefettura, ENAC e Garante per la protezione dei dati personali. Le affermazioni di fatto normativo sono basate sul testo delle fonti primarie citate (leggi, regolamenti, provvedimenti del Garante, sentenze); le ricostruzioni interpretative e i profili di rischio sono indicati come tali nel testo e devono essere valutati con il proprio legale o con il DPO prima di adottare decisioni operative in situazioni ad alto rischio.

Il documento non si sostituisce alla consulenza legale individualizzata. Le verifiche sulle fonti primarie citate sono state effettuate al 1° marzo 2026; la normativa UAS è in rapida evoluzione e richiede monitoraggio continuativo.

Nei casi in cui il quadro normativo presenti orientamenti interpretativi contrapposti — in particolare sulla questione dell'uso dei droni della Polizia Locale per finalità di sicurezza urbana e pubblica sicurezza — il documento espone il dibattito nelle sue componenti essenziali (posizione restrittiva e posizione estensiva), ma le raccomandazioni operative seguono per scelta consapevole l'orientamento oggi più spendibile nei confronti delle autorità di controllo competenti (Garante per la protezione dei dati personali, Ministero dell'Interno, Prefettura). Questo non equivale a un giudizio di infondatezza della tesi estensiva, che rimane argomentabile: equivale a una scelta di gestione del rischio istituzionale nell'attesa di chiarimento legislativo o giurisprudenziale.

1. Il quadro normativo: fonti e gerarchia

1.1 Normativa europea (EASA)

Il diritto UE costituisce la fonte di primo livello per la regolamentazione degli aeromobili senza equipaggio. I regolamenti europei sono direttamente applicabili in tutti gli Stati membri senza necessità di recepimento.

Regolamento (UE) 2018/1139 del Parlamento europeo e del Consiglio del 4 luglio 2018 (GUUE L 212/1), come mod. da Reg. delegato (UE) 2021/1087 e Reg. (UE) 2024/2803

Stabilisce le norme comuni nel settore dell'aviazione civile e istituisce EASA. Quattro articoli/allegati rilevanti per il nostro tema: (1) Art. 2, par. 3, lett. a): il Regolamento NON si applica agli aeromobili "impegnati in operazioni militari, doganali, di polizia, di ricerca e salvataggio, di lotta antincendio, di guardia di frontiera e costiera o in attività o servizi analoghi, effettuati sotto il controllo e la responsabilità di uno Stato membro, nell'interesse pubblico da, o per conto di, un organismo investito dei poteri di autorità pubblica". Questi sono i cc.dd. "voli di Stato" o "voli statali": quando un drone della Polizia Locale agisce con delega formale per finalità di PS, il regime aeronautico si sposta sul diritto nazionale (art. 748 Cod. Nav.); per tutte le altre finalità, si applica il Reg. 2019/947. (2) Art. 56, par. 8: NORMA CHIAVE PER IL DIBATTITO NAZIONALE -- "La presente sezione non pregiudica la possibilità per gli Stati membri di stabilire regole nazionali per subordinare a determinate condizioni l'esercizio di aeromobili senza equipaggio per ragioni che non rientrano nell'ambito di applicazione del presente regolamento, quali la pubblica sicurezza o la tutela della riservatezza". Questa è la base giuridica UE che legittima le scelte del legislatore italiano (D.L. 7/2015 e DM 13.06.2022) di riservare l'uso per PS alle Forze di polizia: non è una limitazione "inventata" dal diritto nazionale, ma una facoltà espressamente attribuita dall'UE agli Stati. (3) Allegato IX, punto 1.1: operatori e piloti remoti devono essere a conoscenza delle norme applicabili in materia di sicurezza, tutela della riservatezza, protezione dei dati, responsabilità civile, assicurazione, security e protezione dell'ambiente. (4) Allegato IX, punto 1.3: gli UAS, se necessario per attenuare i rischi legati alla riservatezza e alla protezione dei dati, devono possedere caratteristiche "che tengono conto dei principi della tutela della riservatezza e della protezione dei dati personali fin dalla progettazione e per impostazione predefinita" (privacy by design e by default). Il privacy by design non è solo un'esigenza GDPR applicata per analogia: è un requisito strutturale del regolamento aeronautico europeo, imposto al costruttore e all'operatore. Rafforza l'obbligo di DPIA anche per droni operanti in Categoria Aperta.

Regolamento delegato (UE) 2019/945 della Commissione (12 mar. 2019)

Definisce i requisiti tecnici per gli UAS (classi da C0 a C6). Tutti gli UAS immessi sul mercato devono rispettare i requisiti della propria classe. I droni di classe C0 (< 250 g) hanno regime semplificato. Aggiornato da Reg. delegato (UE) 2022/1035.

Dal 1° gennaio 2024, tutti i droni delle classi C1 e superiori (e quelli operanti in Categoria Specifica, inclusi i legacy senza marcatura di classe) devono essere dotati di un sistema di identificazione remota (Remote ID) attivo durante il volo, ai sensi del Reg. delegato (UE) 2019/945, art. 11 ss. La registrazione sul portale D-Flight come Operatore UAS è obbligatoria per tutti gli operatori, inclusi i Comuni: in particolare, è obbligatoria anche per i droni di peso inferiore a 250 g se dotati di telecamera, microfono o altri dispositivi di captazione di dati personali; in assenza di tali dispositivi, i droni sotto 250 g sono esenti dall'obbligo di registrazione.

Reg. di esecuzione (UE) 2019/947 della Commissione del 24 maggio 2019 (GUUE L 152 del 11.6.2019), come mod. da Reg. 2020/639, 2020/746, 2021/1166 e 2022/425

Norma cardine sulle regole operative per UAS. Elementi rilevanti verificati sul testo primario: (1) Art. 2 -- assembramenti di persone: definiti come "raduni di persone in cui è impossibile disperdersi a causa dell'elevata densità dei presenti". È una definizione tecnica precisa: non basta un gruppo numeroso, occorre alta densità che impedisca la dispersione. La distinzione è operativamente cruciale: una piazza

animata non è automaticamente un "assembramento"; un corteo mobile o un mercato con percorsi liberi non lo è; al contrario, una partita allo stadio o un concerto con accessi chiusi lo è. (2) Art. 4 + UAS.OPEN.010 -- Categoria Aperta: requisiti tassativi verificati: MTOM < 25 kg; distanza di sicurezza persone; no sorvolo assembramenti; VLOS; max 120 m dal punto più vicino della superficie (non dal livello del mare -- la misura segue la morfologia del terreno: pianure/colline/montagne). Eccezione: in prossimità di ostacoli artificiali alti > 105 m, possibile volare fino a 15 m sopra l'ostacolo su richiesta del gestore (UAS.OPEN.010 par. 3). (3) Art. 14 + Considerando 8 -- obbligo di immatricolazione: gli operatori che usano UAS dotati di "sensori in grado di raccogliere dati personali" (es. videocamera) devono immatricolarsi, a prescindere dal peso del drone. Per la Polizia Locale con videocamera: SEMPRE obbligo di immatricolazione su D-Flight. (4) UAS.OPEN.020 -- esame teorico A1/A3: tra le 40 domande obbligatorie la materia "riservatezza e protezione dei dati" è espressamente prevista come argomento d'esame. Il pilota certificato A1/A3 ha per definizione superato un test su privacy e protezione dati: è un obbligo di legge, non una buona prassi opzionale. (5) Considerando 11 -- doppio ancoraggio art. 56 par. 8 Reg. 2018/1139: il Reg. 2019/947 conferma esplicitamente che le sue norme non pregiudicano la possibilità per gli Stati membri di stabilire regole nazionali per subordinare a determinate condizioni l'esercizio di UAS per ragioni [...] quali la pubblica sicurezza o la protezione della riservatezza e dei dati personali conformemente al diritto dell'Unione.

(6) Reg. 2022/425 -- scadenza scenari standard nazionali: ha prorogato al 1° gennaio 2026 la validità degli scenari standard nazionali IT-STS01 e IT-STS02 (poi confermato da ENAC al 31 dicembre 2025). Dal 1° gennaio 2026 tali scenari sono definitivamente decaduti.

1.2 Normativa nazionale: regolamentazione aeronautica

Regolamento UAS-IT ENAC, Edizione 1 del 4 gennaio 2021 (e aggiornamenti)

Norma integrativa del diritto UE. La Sezione II, Parte B disciplina le operazioni condotte da soggetti pubblici. Art. 27: obbligo di assicurazione RC con massimale minimo 750.000 DSP (~EUR 913.000). Artt. 6 e 9: obbligo di registrazione su D-Flight e QR code su ogni UAS. Obblighi di "occurrence reporting" (safety): in caso di incidente o inconveniente grave, l'operatore deve comunicarlo ad ANSV (Agenzia Nazionale per la Sicurezza del Volo) entro 60 minuti.

IMPORTANTE: dal 1° gennaio 2026 gli scenari nazionali IT-STS01 e IT-STS02 sono decaduti.

Circolare ENAC ATM-09A

Definisce i criteri e le procedure per l'implementazione delle zone geografiche UAS e per la riserva di spazio aereo. È il riferimento operativo principale per la pianificazione del volo: ogni missione deve partire dalla verifica cartografica su D-Flight in base a questa circolare.

Circolare ENAC ATM-03C

Definisce i criteri e le modalità per istituire, modificare e cancellare le zone soggette a restrizioni delle attività di volo. È la fonte operativa per identificare le zone a divieto o restrizione per motivi di sicurezza, ordine pubblico, o protezione di siti sensibili. Va consultata congiuntamente ad ATM-09A nella fase di pianificazione.

Codice della Navigazione (R.D. 30 mar. 1942, n. 327), artt. 743-748 e art. 793 (come sostituito dal D.Lgs. 96/2005 e integrato dal D.Lgs. 151/2006). Testo verificato su fonte primaria (ENAC, fog.it, GU): artt. 743 (nozione; include MAPR), 744 co. 1 (aeromobili di Stato: militari, Forze di polizia Stato, Dogana, VVF, Dipartimento protezione civile – la Polizia Locale non vi rientra), 744 co. 2 (droni Polizia Locale sono aeromobili privati salvo equiparazione), 746 co. 1 (MIT equipara a aeromobile di Stato per servizio di Stato non commerciale), 748 co. 1 (esenzione CdN per Forze di polizia Stato, VVF, equiparati), 793 (divieti di sorvolo ENAC/MIT).

I droni sono aeromobili a tutti gli effetti giuridici (art. 743: include “mezzi aerei a pilotaggio remoto”). — Art. 744 co. 1: sono aeromobili di Stato solo quelli militari e quelli delle Forze di polizia dello Stato, della Dogana, del Corpo nazionale VVF e del Dipartimento della protezione civile. La Polizia Locale non rientra in nessuna di queste categorie: i suoi droni sono aeromobili privati ex art. 744 co. 2, soggetti a tutte le norme del Codice e alla normativa UAS. — Art. 746 co. 1: il Ministero delle Infrastrutture e dei Trasporti (MIT) può equiparare agli aeromobili di Stato quelli “adibiti a un servizio di Stato di carattere non commerciale”. Questa è la base giuridica dei Decreti MIT per la Polizia Locale: solo con il decreto di equiparazione il drone Polizia Locale acquisisce lo status di aeromobile di Stato. — Art. 748 co. 1: l'esenzione dalle norme del Codice vale solo per gli aeromobili militari, di dogana, delle Forze di polizia dello Stato e VVF, e per quelli equiparati ex art. 746. Senza decreto MIT, la Polizia Locale è soggetta all'intero Codice. Con decreto MIT: esenzione dal Codice e da tasse/tariffe aeroportuali (art. 748 co. 2). — Art. 793: ENAC può vietare il sorvolo su zone del territorio per motivi di sicurezza; in presenza di motivi militari, di sicurezza o di ordine pubblico, è tenuta a vietarlo su richiesta della competente amministrazione. Il Ministero delle Infrastrutture e dei Trasporti (MIT) può vietare la navigazione aerea sull'intero territorio per eccezionali motivi di interesse pubblico. [Testo verificato su fonte primaria: fog.it, ENAC, GU; conforme al testo post D.Lgs. 96/2005 e D.Lgs. 151/2006]

1.3 Normativa nazionale: pubblica sicurezza, sicurezza urbana e attribuzioni della Polizia Locale

Legge 7 marzo 1986, n. 65 (Legge quadro Polizia Municipale), artt. 3 e 5

Art. 3: la Polizia Locale collabora con le Forze di polizia dello Stato “previa disposizione del sindaco, quando ne venga fatta, per specifiche operazioni, motivata richiesta dalle competenti autorità”. Art. 5, co. 1: la Polizia Locale esercita nell'ambito territoriale e nei limiti delle proprie attribuzioni: (a) funzioni di PG (agente o ufficiale di PG); (b) polizia stradale; (c) funzioni ausiliarie di pubblica sicurezza “ai sensi dell'articolo 3” -- cioè solo tramite il canale attivato dalla “motivata richiesta” dell’autorità competente (Questore o Prefetto), previa disposizione del Sindaco.

NOTA TECNICA: il meccanismo NON è la “delega del Prefetto” in senso stretto. Il Prefetto non conferisce una “delega” ma formula una “richiesta motivata”; il Sindaco emette la disposizione; solo dopo la Polizia Locale può operare in quella veste. È una distinzione giuridicamente rilevante: manca il nesso di subordinazione diretto che caratterizzerebbe la delega. Art. 5, co. 2: il Prefetto conferisce al personale la qualità di agente di PS previo accertamento dei requisiti.

Art. 5, co. 4:

NORMA RILEVANTE PER I DRONI -- “Nell'esercizio delle funzioni di agente e di ufficiale di polizia giudiziaria e di agente di pubblica sicurezza, il personale di cui sopra, messo a disposizione dal sindaco, dipende operativamente dalla competente autorità giudiziaria o di pubblica sicurezza”. Cioè: durante la missione autorizzata, il Comandante è vincolato alle direttive dell'AG o dell’autorità di PS, non del Sindaco.

QUADRO IN EVOLUZIONE: il DDL C. 1716 (Governo Piantedosi, presentato il 16 feb. 2024, in esame alla I Comm. Camera) prevede una delega al Governo per la riforma organica della L. 65/1986, con criterio direttivo esplicito di ridefinire il rapporto tra funzioni della Polizia Locale e funzioni di PS delle Forze di polizia statali. Fino all'approvazione, la L. 65/1986 rimane l'unico riferimento statale vigente.

D.L. 20 feb. 2017, n. 14, conv. L. 18 apr. 2017, n. 48 (c.d. Decreto Minniti), art. 5 -- Patti per la sicurezza urbana

Disciplina la “sicurezza integrata” e i “Patti per l'attuazione della sicurezza urbana” tra Prefetto e Sindaco. Tra gli obiettivi dei patti rientra esplicitamente l'installazione e gestione di sistemi di videosorveglianza su pubblica via per la prevenzione e il contrasto della criminalità diffusa e predatoria. Il Garante Privacy (Provv. n. 10013356 dell'11 apr. 2024) ha chiarito che: quando un Comune/Polizia Locale presenta un’attività (anche con droni) come finalità di sicurezza urbana, deve dimostrare il titolo istituzionale (patto con Prefettura) e il coordinamento con le autorità competenti; non è sufficiente una delibera o un regolamento interno. La circolare del Ministero dell'Interno del 7 aprile 2025 fornisce indicazioni applicative aggiornate.

Legge 1° aprile 1981, n. 121, art. 16 (Ordinamento Amministrazione PS)

Elenca le Forze di polizia: Polizia di Stato, Arma dei Carabinieri, Guardia di Finanza, Corpo di Polizia Penitenziaria, Corpo Forestale dello Stato (ora nel CC). La Polizia Locale NON è inclusa. Questo è il cardine giuridico della controversia sull’applicabilità del D.M.

13.06.2022 alla Polizia Locale.

D.L. 18 feb. 2015, n. 7, conv. L. 17 apr. 2015, n. 43, art. 5, co. 3-sexies (come sostituito dall'art. 35-sexies D.L. 4 ott. 2018, n. 113, conv. L. 1 dic. 2018, n. 132)

Delega al Ministro dell'Interno di disciplinare le "modalità di utilizzo, da parte delle Forze di polizia, degli aeromobili a pilotaggio remoto" per finalità di PS.

D.M. Interno 13 giugno 2022 (G.U. n. 192 del 18 ago. 2022) - - Decreto attuativo vigente

Campo di applicazione soggettivo (art. 1): UAS "in dotazione o in uso alle Forze di polizia di cui all'art. 16 della legge 1° aprile 1981, n. 121". Finalità (art. 3): controllo del territorio per ordine e sicurezza pubblica, contrasto terrorismo, criminalità organizzata e ambientale. Le modalità operative sono fissate tramite protocolli tecnici tra ciascuna Forze di polizia ed ENAC.

NOTA STORICO-INTERPRETATIVA — Circolare Capo della Polizia n. 555/O.P./0001054/2020/2 del 30 marzo 2020 (Gabrielli)

Nel contesto dell'emergenza COVID-19, il Capo della Polizia confermò con circolare n. 555/O.P./0001054/2020/2 del 30 marzo 2020 (firmata dal Prefetto Gabrielli, indirizzata ai Prefetti e per conoscenza ai Sindaci) che le Polizie locali, non rientrando tra le Forze di polizia ex art. 16 L. 121/1981, **non possono sviluppare autonomamente azioni di controllo del territorio con droni per finalità di pubblica sicurezza**. L'utilizzo eccezionale fu consentito in quella fase esclusivamente previa disposizione del Prefetto, nell'ambito del concorso alle misure emergenziali del D.L. 25 marzo 2020, n. 19 (art. 4, co. 9 — oggi cessato), a tutela del bene giuridico della salute pubblica collettiva (art. 32 Cost.), e limitatamente alle aree e alle modalità indicate dal Prefetto stesso. La circolare ribadiva inoltre che le comunicazioni dei Comuni al Prefetto dovevano includere le aree urbane di impiego, e che il coordinamento avveniva in sede di Comitato Provinciale per l'Ordine e la Sicurezza Pubblica.

Rilievo interpretativo: questa circolare — la fonte istituzionale più autorevole disponibile in materia — conferma a contrario che fuori dal contesto emergenziale straordinario il quadro ordinario è restrittivo. Il principio della riserva di competenza delle Forze di polizia è stato successivamente ribadito dal DM 13 giugno 2022 (vigente) e richiamato espressamente dal Garante Privacy nel provvedimento Treviso 2023. La deroga ENAC allegata alla circolare (nota ENAC prot. 0032363-P del 23/3/2020) era valida fino al 3 aprile 2020 e non ha alcuna valenza operativa residua.

1.4 Giurisprudenza costituzionale: il fondamento della distinzione sicurezza primaria / sicurezza secondaria

La distinzione tra pubblica sicurezza (competenza esclusiva statale ex art. 117, co. 2, lett. h, Cost.) e polizia amministrativa locale (competenza residuale regionale/locale) è elaborata in una linea giurisprudenziale consolidata della Corte costituzionale, che decorre dal 1987 e si consolida con la sent. n. 285/2019. Queste pronunce costituiscono il fondamento giuridico sottostante alle disposizioni normative primarie già esaminate (L. 121/1981, DM 13

giugno 2022, D.L. 14/2017) e ne chiariscono la ratio costituzionale.

C. Cost., sent. 27 marzo 1987, n. 77

Dichiara l'illegittimità costituzionale dell'art. 19, co. 4-5, d.P.R. 616/1977 nella parte in cui i poteri del Prefetto non erano limitati alle sole esigenze di pubblica sicurezza. Fissa il principio: le funzioni di polizia si distinguono in (a) polizia di sicurezza pubblica — di esclusiva competenza statale, attinente alla prevenzione dei reati e al mantenimento dell'ordine pubblico — e (b) polizia amministrativa, trasferibile ad enti locali e regioni nell'ambito delle materie di loro competenza. Solo la prima categoria legittima l'intervento/ingerenza del Prefetto. Implicazione per i droni Polizia Locale: l'uso per finalità di pubblica sicurezza/ordine pubblico è riservato allo Stato; l'uso per finalità di polizia amministrativa locale (accertamenti edilizi, ambiente, ecc.) può rientrare nelle attribuzioni proprie della Polizia Locale. [Testo verificato su giurcost.org]

C. Cost., sent. 25 febbraio 1988, n. 218

Perfeziona la distinzione introdotta dalla n. 77/1987. Definisce l'ordine pubblico come il complesso dei beni giuridici fondamentali e degli interessi pubblici primari — tra cui l'integrità fisica e psichica delle persone, la sicurezza dei possessi e ogni altro bene di fondamentale importanza per l'esistenza e lo svolgimento dell'ordinamento — su cui si regge l'ordinata e civile convivenza dei consociati nella comunità nazionale. Per stabilire se un dato potere di polizia rientri nella competenza statale o in quella locale, occorre applicare un duplice criterio: (a) verificare se la funzione è inerente a una materia di competenza regionale/locale; (b) verificare se gli interessi tutelati sono del tutto interni a quella materia ovvero coinvolgono il nucleo di ordine pubblico di esclusiva spettanza statale. Implicazione per i droni Polizia Locale: l'uso di droni «di sicurezza pubblica in senso stretto» ricade nel nucleo statale; quello per finalità amministrative locali può rientrare nelle attribuzioni della Polizia Locale se non tocca i beni primari dello «ordine pubblico». [Testo verificato su giurcost.org]

C. Cost., sent. 25 luglio 2001, n. 290

Prima pronuncia successiva alla riforma del Titolo V (L. cost. 3/2001) che consolida la distinzione nel nuovo quadro costituzionale. Allo Stato spettano le funzioni e i compiti relativi all'ordine pubblico e alla sicurezza pubblica — intesi come le misure preventive e repressive dirette al mantenimento dell'ordine pubblico, quale «complesso dei beni giuridici fondamentali e degli interessi pubblici primari su cui si regge l'ordinata e civile convivenza nella comunità nazionale» — mentre alle Regioni e agli enti locali spetta la polizia amministrativa, accessoria alle materie di loro competenza. Rientrano in quest'ultima categoria le «misure dirette ad evitare danni o pregiudizi che possono essere arrecati a soggetti giuridici e alle cose nello svolgimento di attività relative alle materie nelle quali vengono esercitate le competenze delle Regioni e degli enti locali, purché non siano coinvolti beni o interessi specificamente tutelati in funzione dell'ordine pubblico e della sicurezza pubblica». Implicazione operativa: il Comune/Polizia Locale che intende usare i droni per finalità di sicurezza deve verificare se l'attività coinvolge beni tutelati dall'ordine pubblico (nel qual caso serve titolo istituzionale ex L. 65/1986 o D.L. 14/2017) oppure rientra nella polizia amministrativa locale (nel qual caso può agire autonomamente nei limiti delle proprie attribuzioni). [Testo verificato su cortecostituzionale.it; conforme a quanto richiamato da C. Cost. n. 167/2010, giurcost.org]

C. Cost., sent. 10 novembre 2011, n. 300

Consolida la definizione restrittiva della materia statale di «ordine pubblico e sicurezza». La Corte ribadisce che la materia statale esclusiva di cui all'art. 117, co. 2, lett. h), Cost. «attiene alla prevenzione dei reati e al mantenimento dell'ordine pubblico, inteso questo quale complesso dei beni giuridici fondamentali e degli interessi pubblici primari sui quali si regge la civile convivenza nella comunità nazionale». Le disposizioni che perseguono finalità di tutela della salute, benessere dei soggetti vulnerabili, quiete pubblica o qualità della vita non rientrano in questo nucleo e rimangono di competenza regionale/locale. Implicazione per i droni Polizia Locale: le attività di volo per finalità di prevenzione/repressione dei reati o mantenimento dell'ordine pubblico restano di competenza statale; le attività per finalità di salute pubblica, ambiente, decoro urbano, sicurezza stradale rientrano nella sfera locale. [Testo verificato su cortecostituzionale.it; richiamata in ex plurimis C. Cost. nn. 35/2011, 167/2010]

C. Cost., sent. 2019, n. 285 — LA PIÙ RILEVANTE PER I DRONI Polizia Locale

Introduce espressamente la distinzione tra «sicurezza in senso stretto (o primaria)» e «sicurezza in senso lato (o secondaria)», divenuta riferimento costante della giurisprudenza costituzionale successiva (richiamata in C. Cost. nn. 236/2020, 69/2023). La **sicurezza primaria** è costituita dalla prevenzione e repressione dei reati («nucleo essenziale») e dalla salvaguardia di beni giuridici fondamentali: è di competenza esclusiva statale ex art. 117, co. 2, lett. h), Cost. e non può essere esercitata da Regioni o enti locali se non nei modi previsti dalla legge statale. La **sicurezza secondaria** è quella «in senso lato»: comprende le politiche e i servizi sociali, la polizia locale, l'assistenza sanitaria, il governo del territorio, la riqualificazione urbana, la prevenzione situazionale (eliminazione fattori di marginalità e degrado). Su questo secondo livello possono intervenire Regioni e Comuni «nell'ambito di competenze ad esse assegnate in via residuale o concorrente». La Corte ha esplicitamente ritenuto compatibili con la Costituzione azioni regionali di prevenzione non coercitiva, formazione professionale condivisa tra Polizia Locale e Forze di polizia, programmi di coesione sociale. APPLICAZIONE AI DRONI: l'uso di droni della Polizia Locale per finalità di sicurezza **primaria** (prevenzione/repressione reati, ordine pubblico) richiede il titolo istituzionale ex L. 65/1986 o D.L. 14/2017 e non può essere esercitato autonomamente (conforme al principio già ribadito dal DM 13 giugno 2022 e dal Garante/Treviso 2023). L'uso per finalità di sicurezza **secondaria** (polizia amministrativa, ambiente, rilievi tecnici, protezione civile) può rientrare nelle ordinarie attribuzioni della Polizia Locale, con i soli obblighi GDPR, aeronautici e di sicurezza sul lavoro. [Testo verificato su cortecostituzionale.it; richiamata in C. Cost. nn. 236/2020, 69/2023, 170/2019]

Linee generali per la promozione della sicurezza integrata — Accordo Conferenza unificata, 24 gennaio 2018

Accordo tra il Governo, le Regioni e gli Enti locali adottato in sede di Conferenza unificata il 24 gennaio 2018, ai sensi dell'art. 2 del D.L. 14/2017 conv. L. 48/2017. Costituisce la «cornice di riferimento delle politiche per la sicurezza integrata» (ANCI). Punto 5 dell'Allegato A — rilevante per la videosorveglianza e per analogia per i droni: «i sistemi di videosorveglianza attivati dalle Forze di polizia rispondono alle finalità di prevenzione generale dei reati e di salvaguardia della sicurezza pubblica» e «sono utilizzabili per finalità di contrasto a fenomeni delittuosi o di prevenzione delle possibili turbative dell'ordine e della sicurezza pubblica di **esclusiva competenza statale** che esorbitano l'ambito della sicurezza urbana». Nota metodologica: le Linee generali confermano che anche nell'ambito della «sicurezza integrata» — che per definizione è cooperativa e multilivello — le finalità di prevenzione/repressione dei reati e di ordine pubblico rimangono di esclusiva competenza statale. Il sistema non autorizza la Polizia Locale ad acquisire autonomamente competenze di sicurezza primaria, ma prevede forme di collaborazione coordinate dalla Prefettura. [Fonte verificata: ANCI; regioni.it; archivio Conferenza unificata; contenuto riprodotto anche su privacy.it (24/01/2018)]

1.5 Iter legislativo per la riforma della L. 65/1986: stato al 1° marzo 2026

AVVERTENZA: Le disposizioni descritte in questa sezione riguardano un iter legislativo ancora in corso al 1° marzo 2026. Nessuna delle proposte di riforma qui illustrate è diritto vigente: le norme applicabili oggi alla Polizia Locale sono esclusivamente quelle indicate nelle sezioni precedenti. Questa sezione ha valore esclusivamente prospettico e di monitoraggio.

La legge quadro 65/1986 è oggetto di un articolato iter di riforma che coinvolge sia la Camera dei deputati (sede principale) sia il Senato. Al 1° marzo 2026 il percorso è in fase avanzata alla Camera ma non ancora concluso. Di seguito il quadro aggiornato verificato sulle fonti primarie (Camera.it, Senato.it).

Atto	Sede / Proponente	Stato al 1° marzo 2026	Rilevanza per i droni Polizia Locale
C. 1716 (testo base)	Camera, Comm. I – Governo (Piantedosi, feb. 2024)	**Testo base adottato il 3 dic. 2025; emendamenti in corso; voto in aula non calendarizzato**	ATTENZIONE: l'art. 1 del C. 1716 mantiene ferma la distinzione Polizia Locale/Forze di polizia ex L. 121/1981. L'eventuale approvazione NON risolverebbe l'ambiguità sull'uso droni per finalità di PS.
S. 883 (abbinato)	Senato, Comm. I – Gasparri (FI, sett. 2023)	Assegnato, esame non ancora iniziato (fonte: senato.it)	Prevede ingresso Polizia Locale nel comparto sicurezza e qualifica come "Forze di polizia del territorio": se approvato aprirebbe spazio per uso droni in finalità PS senza delega prefettizia.
S. 704 (abbinato)	Senato, Comm. I – Romeo (Lega, magg. 2023)	Assegnato, esame non ancora iniziato (fonte: senato.it)	Proposta abrogazione L. 65/1986 e ruolo centrale alle Regioni. Meno rilevante per i droni.

1.6 Normativa sulla protezione dei dati personali

Regolamento (UE) 2016/679 (GDPR) e D.Lgs. 10 agosto 2018, n. 101

Si applica ai trattamenti amministrativi (non di law enforcement). Art. 6, par. 1, lett. e): base giuridica per esercizio di pubblici poteri. Art. 35: DPIA obbligatoria per trattamenti ad alto rischio. Artt. 13-14: informativa agli interessati. Art. 32: misure di sicurezza. Art. 82: diritto al risarcimento del danno da trattamento non conforme. Il Garante Privacy (Delibera n. 467/2018, docweb 9058979) ha pubblicato l'elenco delle tipologie di trattamenti soggetti a DPIA: la videosorveglianza sistematica di aree pubbliche vi rientra espressamente.

D.Lgs. 18 maggio 2018, n. 51 (attuazione Direttiva UE 2016/680)

Si applica ai trattamenti di dati personali effettuati dalle "autorità competenti" a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali. Uno stesso progetto droni può generare entrambi i regimi (GDPR nella fase di monitoraggio amministrativo; D.Lgs. 51/2018 quando si acquisisce una notizia di reato e si opera sotto direzione dell'AG): è necessaria la separazione logica e documentale degli archivi e degli accessi.

1.7 Normativa processuale-penale e penale sostanziale

Codice di procedura penale, art. 234 (Documenti)

Consente l'acquisizione di scritti o altri documenti che rappresentano fatti, persone o cose mediante fotografia, cinematografia, fonografia o qualsiasi altro mezzo. È il canale processuale tipico per l'acquisizione come prova delle immagini e dei video ottenuti dai droni Polizia Locale, quando si tratta di riprese di luoghi pubblici o aperti al pubblico. La Cass. pen., Sez. IV, n. 21557/2024 ha confermato che la videoripresa di luoghi pubblici può essere utilizzata come acquisizione documentale/prova senza automatica assimilazione alle intercettazioni.

Codice di procedura penale, art. 189 (Prove non disciplinate dalla legge)

Il giudice può assumere prove non disciplinate dalla legge se idonee all'accertamento dei fatti e non lesive della libertà morale della persona. È il riferimento normativo sussidiario per alcune forme di videoriprese. Requisiti operativi: delimitare le riprese, documentare i log, assicurare integrità (hash) e catena di custodia, evitare captazioni invasive.

Codice penale, art. 615-bis (Interferenze illecite nella vita privata)

Chiunque, mediante uso di strumenti di ripresa visiva o sonora, si procura indebitamente notizie o immagini attinenti alla vita privata svolgentesi nei luoghi indicati nell'art. 614 c.p. (luoghi di privata dimora) è punito con la reclusione da sei mesi a quattro anni. Se il fatto è commesso da un pubblico ufficiale o incaricato di pubblico servizio con abuso dei poteri o violazione dei doveri inerenti la funzione, la pena è aumentata. La "red line" operativa è netta: il drone non deve mai essere progettato per captare stabilmente l'interno di abitazioni o spazi di vita privata. Le immagini così acquisite, oltre a esporre a responsabilità penale, sarebbero inutilizzabili come prova nel processo.

1.8 Quadro normativo riepilogativo

Fonte normativa	Contenuto rilevante	Impatto sulla Polizia Locale
Reg. (UE) 2018/1139 del 4 luglio 2018 (GUUE L 212/1 del 22.8.2018), come mod. da Reg. delegato (UE) 2021/1087 e Reg. (UE) 2024/2803	Framework EASA per sicurezza aerea civile. Art. 2, par. 3, lett. a): il Regolamento NON si applica agli aeromobili "impegnati in operazioni militari, doganali, di polizia, di ricerca e salvataggio, di lotta antincendio, di guardia di frontiera e costiera [...] effettuati sotto il controllo e la responsabilità di uno Stato membro, nell'interesse pubblico da, o per conto di, un organismo investito dei poteri di autorità pubblica". Art. 56, par. 8: la disciplina UAS "non pregiudica la possibilità per gli Stati membri di stabilire regole nazionali per subordinare a determinate condizioni l'esercizio di aeromobili senza equipaggio per ragioni che non rientrano nell'ambito di applicazione del presente regolamento, quali la pubblica sicurezza o la tutela della riservatezza". Allegato IX, punto 1.3: gli UAS devono incorporare "i principi della tutela della riservatezza e della protezione dei dati personali fin dalla progettazione e per impostazione predefinita" (privacy by design e by default UAS). Allegato IX, punto 1.1: operatori e piloti remoti devono conoscere le norme applicabili "in materia di sicurezza, tutela della riservatezza, protezione dei dati, responsabilità civile, assicurazione, security e protezione dell'ambiente".	Art. 2, par. 3, lett. a): quando la Polizia Locale opera con delega formale per finalità di PS, il regime aeronautico si sposta verso il diritto nazionale (art. 748 Cod. Nav.) anziché il Reg. UE; per tutte le altre finalità si applica il Reg. 2019/947. Art. 56, par. 8: questa norma è la base giuridica UE che legittima le scelte del legislatore italiano (DM 13.06.2022, art. 5 D.L. 7/2015) di riservare l'uso per PS alle Forze di polizia; non è quindi una limitazione "inventata" dal diritto nazionale ma una facoltà espressamente attribuita dall'UE agli Stati. Allegato IX, punto 1.3: il privacy by design non è solo un'esigenza GDPR applicata per analogia, ma un requisito strutturale del regolamento aeronautico europeo -- il costruttore e l'operatore sono obbligati a implementarlo; rafforza l'obbligo di DPIA anche per droni in Categoria Aperta.
Reg. UE 2019/945	Classi e requisiti tecnici degli UAS (C0-C6)	I droni acquistati dalla Polizia Locale devono rispettare la classe appropriata per le operazioni pianificate
Reg. di esecuzione (UE) 2019/947 della Commissione del 24 mag. 2019 (GUUE L 152/45 del 11.6.2019), come mod. da Reg. 2020/639, 2020/746, 2021/1166 e 2022/425	Norma cardine sulle regole operative per UAS. Art. 2: definizioni operative chiave. "Assembramenti di persone": definiti come "raduni di persone in cui è impossibile disperdersi a causa dell'elevata densità dei presenti" -- NON qualsiasi gruppo di persone, solo raduni ad alta densità non mobili. Art. 4: Categoria Aperta -- requisiti tassativi: (1) MTOM < 25 kg; (2) distanza di sicurezza dalle persone; (3) no sorvolo assembramenti; (4) VLOS costante; (5) max 120 m dal punto più vicino della superficie terrestre; (6) no merci pericolose. Art. UAS.OPEN.010 par. 2: il limite di 120 m si misura dal punto più vicino della superficie, adeguandosi alla morfologia del terreno (pianure/colline/montagne). Par. 3: in prossimità di ostacoli artificiali alti (> 105 m), è possibile volare fino a 15 m sopra l'ostacolo su richiesta del gestore. Art. 15: gli Stati membri possono definire zone geografiche UAS e vietare/condizionare operazioni per ragioni di sicurezza, riservatezza, ambiente. Art. 14: obbligo di immatricolazione per operatori che usano UAS dotati di sensori in grado di raccogliere dati personali. UAS.OPEN.020: esame A1/A3 comprende obbligatoriamente la materia "riservatezza e protezione dei dati". Considerando 11: conferma esplicita che il Reg. "non pregiudica la possibilità per gli Stati membri di stabilire regole nazionali per subordinare a determinate condizioni l'esercizio di UAS per ragioni [...] quali la pubblica sicurezza o la protezione della riservatezza e dei dati personali" -- doppio ancoraggio con art. 56 par. 8 Reg. 2018/1139. IT-STS01 e IT-STS02: Reg. 2022/425 ha prorogato al 1.1.2026; da tale data i scenari standard nazionali non sono più utilizzabili (confermato da ENAC).	La Polizia Locale opera normalmente in Categoria Aperta (A1/A2/A3) o Specifica; deve rispettare VLOS, MTOM, altitudine max 120 m (misurata dalla superficie, non dal livello del mare), divieti su assembramenti. PRECISIONE OPERATIVA: la Polizia Locale può volare sopra persone isolate (sottocategoria A1 con C0/C1); in A2 distanza minima 30 m (o 5 m con modalità bassa velocità); in A3 almeno 150 m da aree abitate. "Assembramento" ha definizione tecnica precisa: non basta un gruppo numeroso ma occorre densità tale da impedire la dispersione. Art. 14 + Considerando 8: il Comune/operatore che usa UAS con videocamera (sensore di raccolta dati personali) ha SEMPRE obbligo di immatricolazione su D-Flight, a prescindere dal peso. UAS.OPEN.020: il pilota che supera l'esame A1/A3 ha per definizione studiato privacy e protezione dati -- ciò è obbligatorio per legge, non facoltativo.
Regolamento UAS-IT ENAC (4 gen. 2021)	Normativa nazionale integrativa; Sezione II Parte B per operatori UAS pubblici; art. 27: assicurazione RC obbligatoria; obblighi occurrence reporting con notifica ANSV entro 60 minuti in caso di incidente/inconveniente grave	Obbligo di registrazione su D-Flight, attestato pilota, assicurazione RC, notifica ANSV per incidenti
Codice della Navigazione (R.D. 30 mar. 1942, n. 327),	I droni sono aeromobili a tutti gli effetti; art. 793: ENAC può vietare il sorvolo e, su richiesta della competente amministrazione per motivi militari/sicurezza/ordine	Obbligo di verifica prevolo delle zone a divieto di sorvolo ex art. 793; per tali aree servono autorizzazione ENAC + nulla osta del

Fonte normativa	Contenuto rilevante	Impatto sulla Polizia Locale
artt. 743-748 e art. 793 (come sost. dal D.Lgs. 96/2005)	pubblico, il divieto è obbligatorio; MIT può vietare navigazione aerea per eccezionali motivi di interesse pubblico	gestore/proprietario del sito (modalità operative: Circolare ENAC ATM-03C)
D.L. 18 feb. 2015, n. 7, conv. L. 17 apr. 2015, n. 43, art. 5, co. 3-sexies (mod. art. 35-sexies D.L. 113/2018 conv. L. 132/2018)	Delega al Ministero dell'Interno per disciplinare l'uso dei droni “da parte delle Forze di polizia” ai fini di pubblica sicurezza	Le Polizia Locale non rientrano nell'art. 16 L. 121/1981; il DM attuativo non si applica loro direttamente
D.M. Interno 13 giu. 2022 (G.U. 18 ago. 2022, n. 192)	Modalità di utilizzo UAS da parte delle Forze di polizia ex art. 16 L. 121/1981 (PS, CC, GdF, Penitenziaria, Forestale)	Interpretazione controversa: Prefettura di Lecce (feb. 2026) e Min. Interno: riserva alle Forze di polizia; ANVU: il DM regola le modalità operative per le Forze di polizia, non introduce divieto assoluto per la Polizia Locale
L. 7 mar. 1986, n. 65 (Legge quadro PM), artt. 3, 5 co. 1 e 4	Art. 3: la Polizia Locale collabora con le Forze di polizia dello Stato “previa disposizione del sindaco, quando ne venga fatta, per specifiche operazioni, motivata richiesta dalle competenti autorità”. Art. 5, co. 1: la Polizia Locale esercita: (a) funzioni di PG; (b) polizia stradale; (c) funzioni ausiliarie di PS “ai sensi dell'articolo 3” -- cioè solo tramite il canale della richiesta motivata. NOTA: il meccanismo NON è la “delega del Prefetto” in senso tecnico, ma la “motivata richiesta” dell’autorità (Questore o Prefetto), previa disposizione del Sindaco -- distinzione rilevante. Art. 5, co. 4: durante l'esercizio di tali funzioni ausiliarie, il personale Polizia Locale “messo a disposizione dal sindaco, dipende operativamente dalla competente autorità giudiziaria o di pubblica sicurezza”. Art. 5, co. 2: il Prefetto conferisce la qualità di agente di PS previa verifica dei requisiti.	Canale giuridico principale per l'uso dei droni in finalità ausiliarie di PS: serve (1) richiesta motivata del Questore/Prefetto per specifiche operazioni; (2) disposizione del Sindaco; (3) messa a disposizione formale del personale. Art. 5, co. 4: durante quella missione, il Comandante risponde all'AG/autorità PS, non al Sindaco -- con implicazioni sulla catena di comando, sulla titolarità del trattamento dati (art. 4 GDPR), e sulla catena di custodia delle prove. NOTA: DDL C. 1716 (Governo Piantedosi, pres. 16 feb. 2024, in Comm. Camera) propone riforma organica della L. 65/1986: tra i criteri direttivi, la ridefinizione del rapporto Polizia Locale/Forze di polizia statali. Fino all'approvazione, la legge del 1986 rimane l'unico riferimento statale.
D.L. 20 feb. 2017, n. 14, conv. L. 18 apr. 2017, n. 48 (c.d. Decreto Minniti), art. 5	Disciplina i “Patti per l'attuazione della sicurezza urbana” tra Prefetto e Sindaco; include tra gli obiettivi l'installazione di sistemi di videosorveglianza per prevenzione/contrasto criminalità diffusa e predatoria su pubblica via; la Circolare del Ministero dell’Interno, Gabinetto del Ministro, Ufficio II – Ordine e Sicurezza Pubblica, circolare prot. 11001/123/111 (3), prot. uscita n. 0031004 del 7 aprile 2025, recante indicazioni applicative sui Patti per l’attuazione della sicurezza urbana e l’installazione di sistemi di videosorveglianza	Secondo canale formale (alternativo/complementare alla delega ex L. 65/1986) per progetti di sicurezza urbana con droni: se l'uso è qualificato come sicurezza urbana, serve il Patto Prefetto-Sindaco. Il Garante (Provv. n. 10013356/2024) ha ribadito che non basta una delibera interna del Comune
Reg. UE 2016/679 (GDPR) e D.Lgs. 101/2018	Protezione dati personali; art. 35 obbligo DPIA per trattamenti ad alto rischio; art. 6 basi giuridiche; artt. 13-14 informativa; art. 32 misure di sicurezza; art. 82 diritto al risarcimento del danno	La Polizia Locale deve individuare la base giuridica del trattamento ai sensi dell’art. 6, par. 1, lett. e) GDPR e condurre la DPIA quando il trattamento presenta un rischio elevato; nella prassi operativa della Polizia Locale, la DPIA è normalmente necessaria negli impieghi con telecamera che comportano monitoraggio sistematico o ricorrente di aree accessibili al pubblico. I soggetti danneggiati da un trattamento illecito hanno diritto al risarcimento
D.Lgs. 18 mag. 2018, n. 51	Trattamento dati per finalità di prevenzione, indagine e perseguimento reati da parte di “autorità competenti”	Se i voli perseguono finalità di accertamento illeciti penali, si applica il D.Lgs. 51/2018; la DPIA va inviata preventivamente al Garante (solo in presenza di rischio residuo elevato non mitigabile); separare archivi e accessi rispetto ai trattamenti ex GDPR
Codice di procedura penale, artt. 234 e 189	Art. 234: acquisizione di scritti o altri documenti che rappresentano fatti/persone/cose tramite fotografia, cinematografia o qualunque mezzo; art. 189: prove non disciplinate dalla legge, ammissibili se idonee all'accertamento e non lesive della libertà morale	Le riprese video dall'alto di aree pubbliche sono tipicamente acquisibili come prova documentale ex art. 234 c.p.p. (non come intercettazioni); essenziale: integrità del file, hash, log e catena di custodia

Fonte normativa	Contenuto rilevante	Impatto sulla Polizia Locale
Codice penale, art. 615-bis (Interferenze illecite nella vita privata)	Chiunque, mediante uso di strumenti di ripresa visiva o sonora, si procura indebitamente notizie o immagini attinenti alla vita privata svolgentesi nei luoghi indicati nell'articolo 614 è punito con la reclusione	Il drone che sorvolasse stabilmente o captasse l'interno di abitazioni o spazi di vita privata senza autorizzazione dell'autorità giudiziaria espone l'operatore e i responsabili a responsabilità penale; le immagini così acquisite sarebbero inutilizzabili come prova
D.Lgs. 9 apr. 2008, n. 81 (Testo Unico Sicurezza sul Lavoro)	Si applica a TUTTI i settori di attività, pubblici e privati, e a tutte le tipologie di rischio, incluso l'uso di attrezzature da lavoro quali i droni. Obblighi principali: (1) Documento di Valutazione dei Rischi (DVR) specifico per l'attività con UAS, comprendente: rischi elettromagnetici, stanchezza visiva del pilota, condizioni meteorologiche operative, emergenze a terra; (2) formazione e addestramento specifico del lavoratore-pilota; (3) sorveglianza sanitaria se esposizione a rischi specifici; (4) designazione del RSPP (Responsabile Servizio Prevenzione e Protezione); (5) art. 36-37: informazione e formazione sufficiente e adeguata per ogni mansione prima dell'operatività	Il Comune che impiega un agente come pilota UAS è DATORE DI LAVORO ai sensi del D.Lgs. 81/2008 e deve: (a) includere l'attività con droni nel DVR del Comando (non è facoltativo); (b) formare il pilota specificamente sui rischi dell'attività; (c) verificare l'idoneità sanitaria se richiesta. Questo adempimento è DISTINTO e AUTONOMO rispetto a tutti gli altri (GDPR, aeronautica, privacy): riguarda la tutela del lavoratore-pilota, non delle terze persone riprese. In caso di infortunio del pilota durante il volo, la PA risponde ex D.Lgs. 81/2008 se non ha adottato tutte le misure di protezione.
WP29 (Gruppo di Lavoro art. 29), Parere 01/2015 sulla privacy e l'uso dei droni (01673/15/IT WP231), adottato il 16 giu. 2015	Unico documento istituzionale europeo dedicato specificamente all'uso di droni per il contrasto penale. Inquadramento temporale: adottato nel regime della Direttiva 95/46/CE (ora abrogata); parzialmente aggiornato dalle Linee Guida EDPB 3/2019 per i profili GDPR-videosorveglianza. Rimane l'unico riferimento europeo specifico per droni-contrasto. Il WP29 è stato sostituito dall'EDPB il 25 maggio 2018 (entrata in vigore GDPR), ma i suoi orientamenti restano validi come fonte interpretativa. PAR. 3.2 (contrasto penale): "l'uso di droni utilizzati direttamente dalla polizia [...] dà origine a rischi elevati per i diritti e le libertà delle persone e interferisce direttamente con i diritti al rispetto della vita privata"; uso ammesso solo se: (1) valida base giuridica; (2) necessità e adeguatezza dimostrata; (3) proporzionalità; (4) motivazione che giustifichi per quale ragione strumenti meno intrusivi non possono conseguire lo stesso obiettivo. PAR. 5.4 (Raccomandazioni contrasto): (1) principi di necessità, proporzionalità, limitazione finalità, minimizzazione, privacy by design; (2) termine di conservazione rigoroso; (3) trasparenza e informativa agli interessati; (4) no rintracciamento costante, salvo indagini autorizzate; (5) attrezzatura adeguata alle finalità (no sovradimensionamento tecnologico); (6) divieto decisioni automatizzate -- SEMPRE controllo umano prima di qualsiasi decisione su individui; (7) riesame giudiziario possibile; (8) riesame periodico di necessità e conformità; (9) approvazione gerarchica superiore per indagini di sorveglianza; (10) dati inseriti nei fascicoli amministrativi utilizzabili in tribunale.	Il Parere WP29 01/2015 funge da riferimento per il disciplinare operativo interno: la Polizia Locale che intende usare droni per finalità di contrasto deve predisporre un regolamento operativo che rispetti le 10 condizioni del §5.4. In particolare: (a) MOTIVAZIONE SCRITTA che dimostri perché strumenti meno invasivi non sufficienti (obbligatoria ad ogni missione o tipologia di missione); (b) CONSERVAZIONE MINIMA: termine rigoroso e giustificato, non più lungo del necessario; (c) INFORMATIVA PUBBLICA: gli interessati devono poter conoscere le modalità del trattamento (cartelli, pubblicazione su sito, ecc.); (d) APPROVAZIONE GERARCHICA AUMENTATA: le missioni di sorveglianza di persone richiedono autorizzazione a livello gerarchico superiore rispetto ai voli amministrativi; (e) NESSUNA DECISIONE AUTOMATICA: qualsiasi misura su un individuo richiede sempre il filtro umano.
Garante Privacy, Delibera n. 467 dell'11 ott. 2018 (docweb 9058979, G.U. n. 269/2018)	Elenco tassativo delle tipologie di trattamenti soggetti a DPIA obbligatoria ex art. 35, par. 4, GDPR. Categorie rilevanti per i droni: (1) trattamenti sistematici per osservazione/monitoraggio/controllo degli interessati; (2) trattamenti di dati su condanne penali/reati interconnessi con altri dati; (3) sistemi tecnologici in ambito lavorativo dai quali derivi possibilità di controllo a distanza dei dipendenti; (4) trattamenti non occasionali di dati di soggetti vulnerabili; (5) raccolta dati tramite reti (streaming video). L'elenco non è esaustivo: DPIA obbligatoria anche quando ricorrono 2 o più criteri WP248 rev. 01	Fonte primaria italiana per determinare l'obbligatorietà della DPIA: per i droni della Polizia Locale, nella pratica quasi ogni volo ricorrente o sistematico ricade in almeno due categorie (uso nuove tecnologie + monitoraggio aree pubbliche). La Delibera costituisce la base formale per l'obbligo di DPIA nel regolamento interno della Polizia Locale
Garante Privacy, Provv. n. 405 del 4 lug. 2024 (Comune di Treviso, docweb 10050298)	DRONI: archiviazione del procedimento (uso avvenuto in supporto alle Forze di polizia, violazione non comprovata), ma con statuizione di principio: "il quadro normativo di settore non consente in via generale alle Polizie Locali di impiegare droni dotati di dispositivi video per finalità connesse alla tutela della pubblica sicurezza" (art. 3 DM	Doppio precedente: (1) principio di diritto sul divieto implicito alla Polizia Locale per uso droni per PS; (2) chiarimento che anche sagome termiche indistinguibili possono essere dati personali. L'archiviazione non equivale a via libera: significa solo che nel caso concreto la

Fonte normativa	Contenuto rilevante	Impatto sulla Polizia Locale
	13.06.2022 richiamato espressamente). Afferma che anche le mappe di calore termiche possono comportare trattamento di dati personali, anche relativi a reati. APP TrevisoSicura: SANZIONE EUR 7.000 per violazioni GDPR (assenza base giuridica, informativa inidonea). ATTENZIONE: fonte AI spesso attribuisce erroneamente la sanzione ai droni	violazione non era comprovata; il principio di diritto enunciato rimane vincolante come indirizzo interpretativo
Garante Privacy, Provv. n. 10013356 dell'11 apr. 2024 (caso telecamera comunale)	Il Garante ribadisce che la Polizia Locale non ha competenze generali di pubblica sicurezza; richiama L. 65/1986 e la necessità del Patto Prefetto-Sindaco ex D.L. 14/2017 per videosorveglianza su pubblica via legata a sicurezza urbana; non basta una delibera/regolamento interno del Comune	Applicabile per analogia ai droni: quando un Comune/Polizia Locale presenta i droni come strumento di “sicurezza pubblica/urbana”, deve dimostrare il titolo e il coordinamento istituzionale con la Prefettura
Garante Privacy, Provv. n. 10198694 (Comune di Orte)	Sanzione e rilievi specifici su: DPIA mancante ex art. 35 GDPR e periodo di conservazione dei dati non conforme ai principi di limitazione	Secondo precedente sanzionatorio (distinto da Treviso) che conferma: la DPIA e la retention policy non sono adempimenti accessori ma condizioni di liceità del trattamento
Cass. pen., Sez. IV, sent. n. 21557/2024	Tratta l’utilizzabilità di videoriprese effettuate in luoghi pubblici/aperti al pubblico; conferma che la videoripresa su luogo pubblico può essere utilizzata come acquisizione documentale/prova senza automatica assimilazione alle intercettazioni, con le dovute cautele del caso	Le riprese drone su aree pubbliche per documentare fatti (dinamica sinistro, abbandono rifiuti) sono tendenzialmente ammissibili come prova; essenziale delimitare le riprese, documentare i log e garantire integrità e catena di custodia
Cass. pen., Sez. III, sent. n. 50919/2019	Conferma la rilevanza penale in caso di videosorveglianza lavorativa in violazione delle garanzie di legge (Statuto dei Lavoratori, art. 4 L. 300/1970)	Alert per impieghi drone in prossimità di strutture comunali, cantieri o servizi con personale: l'uso deve escludere il controllo a distanza dei lavoratori; necessaria formazione specifica e previsione espressa nel regolamento interno
D.P.R. 15 gennaio 2018, n. 15 (G.U. n. 61 del 14 marzo 2018, in vigore dal 29 marzo 2018), artt. 1 c. 3, 6 cc. 1-2, 22, 23 cc. 3-4 e 24 cc. 4-5	Art. 1, c. 3: il D.P.R. si applica esclusivamente agli organi ex art. 57 D.Lgs. 196/2003 (Forze di polizia ex art. 16 L. 121/1981) -- la Polizia Locale è espressamente esclusa dall'ambito applicativo diretto. Art. 23, c. 3: il trattamento dati via APR è classificato tra quelli a “rischi specifici” ex art. 6, per la loro “potenziale invasività”. Art. 23, c. 4: l'uso di sistemi di ripresa su APR è autorizzato al livello gerarchico non inferiore a capo ufficio o comandante di reparto. Artt. 6, c. 2 e 24, c. 4 (non art. 23 come riportato in alcune fonti secondarie): file di log non modificabili, conservati per 5 anni dall'accesso o dall'operazione, accessibili solo per verifica liceità del trattamento, controllo interno e procedimento penale.	NON applicabile direttamente alla Polizia Locale (art. 1, c. 3 espresso). Rilevante come parametro interpretativo e standard di buona prassi per: (a) classificazione del trattamento drone come ad alto rischio -> obbligo DPIA ex art. 35 GDPR; (b) soglia gerarchica minima di autorizzazione per uso APR con sensori; (c) standard tecnici per file di log da recepire nel regolamento interno della Polizia Locale
Prefettura di Lecce, nota prot. 0024109 del 12 feb. 2026 (dopo interlocuzione con Min. Interno - DPS)	Afferma che l'art. 5, co. 3-sexies D.L. 7/2015 circoscrive l'uso dei droni “alle sole Forze di polizia ex art. 16 L. 121/1981”, escludendo la Polizia Locale	Orientamento restrittivo più recente del Ministero dell'Interno; in via di massima prudenza, la Polizia Locale deve ottenere delega formale per ogni uso in finalità di PS
ANVU (Associazione Professionale Polizia Locale d'Italia), documento 18 feb. 2026	Contesta la nota della Prefettura di Lecce; argomenta che il DM 13.06.2022 regola le “modalità” operative senza introdurre un divieto assoluto per la Polizia Locale; i limiti reali sono di natura aeronautica, GDPR e costituzionale	Posizione contraria: la Polizia Locale può usare droni nell'esercizio delle proprie competenze istituzionali senza necessità di “monopolio tecnologico” delle Forze di polizia

2. La questione centrale: le polizie locali possono usare i droni?

2.1 La posizione restrittiva (Ministero dell'Interno / Garante Privacy)

L'interpretazione più restrittiva si fonda su tre precedenti autorevoli (due provvedimenti del Garante e la nota prefettizia del 2026).

Garante Privacy, Provvedimento n. 405 del 4 luglio 2024 (Comune di Treviso, docweb 10050298)

FATTI: La Polizia Locale di Treviso ha impiegato droni dotati di telecamere termiche per generare mappe di calore ("sagome indistinguibili") al fine di guidare le pattuglie nel contrasto ai furti notturni. Il Comune ha sostenuto che le termocamere non identificano i soggetti e che nessun dato personale viene raccolto.

PRONUNCIA SUL MERITO DRONI: Il Garante ha rigettato la tesi del Comune affermando che "l'impiego di droni dotati di telecamere termiche, al fine di generare c.d. mappe di calore, sulla base delle quali possono essere disposti controlli de visu da parte delle pattuglie della Polizia locale in servizio sul territorio, può comportare un trattamento di dati personali, anche relativi a reati".

STATUIZIONE FONDAMENTALE SUL DIVIETO IMPLICITO ALLA Polizia Locale: Il Garante ha affermato espressamente che "l'art. 3 del decreto del Ministero dell'interno del 13 giugno 2022 prevede che le Forze di polizia impiegano gli UAS ai fini del controllo del territorio per finalità di ordine e sicurezza pubblica. Il quadro normativo di settore non consente, pertanto, in via generale alle Polizie locali dei Comuni di impiegare droni, dotati di dispositivi video, per finalità connesse alla tutela della pubblica sicurezza" (fatti salvi i casi di delega per specifiche operazioni).

ESITO DIFFERENZIATO (ATTENZIONE -- fonte AI spesso confonde): (a) Sul profilo DRONI: archiviazione, perché nel caso concreto l'uso era avvenuto in supporto alle Forze di polizia e non risultava comprovata la violazione. (b) Sul profilo APP "TrevisoSicura": SANZIONE di EUR 7.000 per violazioni GDPR (assenza di base giuridica, informativa inidonea).

IMPLICAZIONE OPERATIVA: Il Garante ha ricostruito il quadro normativo in modo da escludere la Polizia Locale dall'uso autonomo dei droni per finalità di PS/ordine pubblico, citando direttamente il DM 13.06.2022. La conclusione con archiviazione NON significa via libera: significa solo che in quel caso specifico il profilo illiceità non era sufficientemente comprovato. Il principio di diritto enunciato rimane a tutti gli effetti un precedente di indirizzo.

Garante Privacy, Provvedimento n. 10013356 dell'11 aprile 2024 (caso telecamera comunale)

In un caso su videosorveglianza comunale invocando pubblica sicurezza/accertamento reati, il Garante ha ribadito che la Polizia Locale non ha competenze generali di pubblica sicurezza e richiama la necessità del Patto Prefetto-Sindaco ex D.L. 14/2017 per la videosorveglianza su pubblica via per finalità di sicurezza urbana. Implicazione diretta per i droni: quando un Comune/Polizia Locale presenta i droni come strumento di sicurezza pubblica/urbana, deve dimostrare titolo e coordinamento istituzionale, non basta una delibera o un regolamento interno.

Prefettura di Lecce, nota prot. 0024109 del 12 febbraio 2026 (dopo interlocuzione con Min. Interno - DPS)

In risposta a una richiesta su uso di droni dalla Polizia Locale (per abbandono rifiuti e abusivismo edilizio), la Prefettura, riportando l'orientamento del Ministero dell'Interno, ha affermato che l'art. 5, co. 3-sexies D.L. 7/2015 circoscrive la facoltà di impiego dei droni "alle sole Forze di polizia ex art. 16 L. 121/1981", escludendo la Polizia Locale. È la posizione istituzionale più recente del Ministero dell'Interno.

> **⚠ ATTENZIONE**
> RISCHIO CONCRETO: L'uso non autorizzato di droni per attività di PS o sicurezza urbana senza Patto Prefetto-Sindaco o delega formale espone i funzionari responsabili a potenziali profili di responsabilità personale. Sul piano GDPR, il Garante ha già sanzionato enti locali (Treviso, Orte). Sul piano penale, l'uso improprio verso aree private configura il reato ex art. 615-bis c.p. Sul piano contabile, acquisti e gestione non conformi possono determinare responsabilità erariale davanti alla Corte dei conti.

2.2 La posizione estensiva (ANVU e dottrina)

L'Associazione Professionale Polizia Locale d'Italia (ANVU), con un articolato documento del 18 febbraio 2026, ha contestato la nota della Prefettura di Lecce sul piano giuridico, avanzando le seguenti argomentazioni:

- Il D.M. 13 giu. 2022 disciplina le "modalità" di utilizzo dei droni "da parte delle Forze di polizia", non introduce un "divieto assoluto" per altri soggetti.
- I droni sono strumenti di libera vendita; sarebbe paradossale che proprio la Polizia Locale -- istituzionalmente preposta alla vigilanza e all'accertamento dei reati -- fosse esclusa dall'uso di uno strumento liberamente disponibile.
- La Polizia Locale svolge funzioni di polizia giudiziaria (art. 5, co. 1, lett. b) L. 65/1986) e funzioni di vigilanza su normativa di settore (edilizia, ambiente, commercio). In tale veste, l'uso di strumenti di documentazione è strumentale all'esercizio di competenze proprie, non di PS.
- I limiti reali all'uso dei droni da parte della Polizia Locale sono di natura aeronautica (rispetto del Reg. UE 2019/947, Reg. UAS-IT ENAC), di protezione dati (GDPR, DPIA), costituzionale (proporzionalità, inviolabilità domicilio) e processuale (art. 615-bis c.p., inutilizzabilità della prova); non esistono "divieti assoluti soggettivi".
- A livello UE, il Reg. 2018/1139, art. 56, par. 8, conferisce esplicitamente agli Stati membri la facoltà di "stabilire regole nazionali per subordinare a determinate condizioni l'esercizio di aeromobili senza equipaggio per ragioni [...] quali la pubblica sicurezza": ciò significa che il DM 13.06.2022 esercita una facoltà UE, non impone un divieto assoluto; i limiti alle modalità operative non equivalgono a un divieto soggettivo della Polizia Locale. (La posizione restrittiva replica che la medesima norma attribuisce tale facoltà agli Stati, che l'hanno esercitata riservando l'uso alle Forze di polizia -- non a qualunque corpo di polizia.)

2.3 La distinzione cruciale: finalità amministrativa vs. sicurezza urbana vs. pubblica sicurezza

La matrice sotto riportata individua tre livelli distinti, ciascuno con i propri requisiti di legittimità.

FINALITÀ AMMINISTRATIVA	SICUREZZA URBANA	PUBBLICA SICUREZZA
• Accertamento abusi edilizi • Rilievo sinistri in zone impervie • Discariche abusive in aree remote • Monitoraggio ambiente • Protezione civile, dispersi • Ispezione infrastrutture • Incendi in aree boschive • Rilievi tecnici/aerofotogrammetrici	• Prevenzione criminalità diffusa/predatoria • Sorveglianza su pubblica via **Richiede:** • Patto Prefetto-Sindaco ex D.L. 14/2017 • Governance privacy documentata • DPIA + informativa	• Contrasto terrorismo, criminalità organizzata • Ordine pubblico • Attività Forze di polizia ex art. 16 L. 121/1981 **Richiede:** • Delega formale Prefetto/Questore ex L. 65/1986 • Coordinamento Forze di polizia • DPIA + D.Lgs. 51/2018
Regime: GDPR + normativa aeronautica. DPIA spesso necessaria.	*Regime: GDPR con vincoli istituzionali. Patto Prefetto-Sindaco + DPIA.*	*Regime: D.Lgs. 51/2018. Delega formale obbligatoria. DPIA preventiva al Garante solo in presenza di rischio residuo elevato non mitigabile.*

3. Profili di protezione dei dati personali

WP29 (Gruppo di Lavoro art. 29), Parere 01/2015 "privacy e utilizzo di droni" (01673/15/IT WP231) -- adottato il 16 giugno 2015

INQUADRAMENTO: Il WP29 è stato sostituito dall'EDPB il 25 maggio 2018 (entrata in vigore del GDPR). Questo parere risale al regime della Direttiva 95/46/CE, ed è stato parzialmente aggiornato dalle Linee Guida EDPB 3/2019 per i profili di videosorveglianza generale. Tuttavia, rimane L'UNICO DOCUMENTO ISTITUZIONALE EUROPEO specificamente dedicato all'uso di droni per il contrasto penale; nessun aggiornamento EDPB ha trattato questo tema con pari specificità. I suoi principi restano validi come orientamento interpretativo e sono richiamati dalla dottrina e dalla giurisprudenza italiane in materia di droni. PAR. 3.2 -- DRONI PER IL CONTRASTO PENALE: il WP29 avverte che l'uso di droni da parte della polizia e di altre autorità di contrasto dà origine a rischi elevati per i diritti e le libertà delle persone. L'uso da parte di autorità di contrasto è ammissibile solo se: (1) esiste una valida base giuridica; (2) i droni sono usati solo dove vi sia dimostrazione concreta della loro necessità e adeguatezza per le finalità specifiche; (3) il trattamento rispetta il principio di proporzionalità; (4) sono motivate le ragioni per cui strumenti meno intrusivi non possono conseguire lo stesso obiettivo. Il WP29 richiama espressamente l'art. 52 della Carta dei diritti fondamentali UE e l'art. 8, par. 2, CEDU. PAR. 5.4 -- DIECI CONDIZIONI OPERATIVE PER IL CONTRASTO: (1) necessità, proporzionalità, limitazione finalità, minimizzazione dati, privacy by design; (2) termine di conservazione rigoroso e giustificato; (3) trasparenza: il trattamento deve essere per legge trasparente e prevedibile per gli interessati; (4) no rintracciamento costante degli individui, salvo indagini autorizzate con attrezzatura adeguata alle finalità; (5) divieto di esecuzione automatizzata delle decisioni -- SEMPRE controllo umano prima di qualsiasi decisione che possa avere ripercussioni su un individuo; (6) possibilità di riesame giudiziario dell'uso a fini di intelligence e contrasto; (7) riesame periodico della necessità del trattamento e della conformità ai quadri giuridici in evoluzione; (8) approvazione gerarchica a livello sufficientemente elevato per operazioni di sorveglianza; (9) dati raccolti inseriti nei fascicoli amministrativi utilizzabili in tribunale; (10) conformità alla Convenzione n. 108 del Consiglio d'Europa e alla Raccomandazione R(87)15 sul trattamento dati nel settore della polizia.

3.0 Schema decisionale: quale regime privacy si applica al volo?

Prima di qualsiasi missione con drone dotato di sensori, il Comandante (o il DPO) deve determinare quale regime di protezione dei dati si applica. La risposta dipende dalla finalità concreta del volo, non dall'identità del soggetto che lo esegue. Lo schema seguente è una guida operativa. In caso di dubbio sulla classificazione, applicare il regime più restrittivo (INTERPRETAZIONE).

Finalità concreta del volo	Regime normativo applicabile	Valutazione di impatto (DPIA)	Consultazione preventiva del Garante	Documentazione minima da conservare
Finalità amministrativa pura (rilievi edilizi, ambientali, sinistri stradali, monitoraggi tecnici, accertamenti di competenza comunale non connessi a reati)	Reg. (UE) 2016/679 (GDPR) + D.Lgs. 101/2018	Obbligatoria quando il trattamento presenta un rischio elevato per i diritti e le libertà delle persone fisiche (art. 35 GDPR). La videosorveglianza sistematica di aree accessibili al pubblico rientra tra i trattamenti individuati dal Garante (Delibera n. 467/2018, docweb 9058979).	Obbligatoria solo se, all'esito della DPIA, residua un rischio elevato non mitigabile (art. 36 GDPR).	DPIA; atto amministrativo che individua finalità e base giuridica (art. 6, par. 1, lett. e) GDPR); registro missioni; log accessi; misure di sicurezza; policy di conservazione.
Sicurezza urbana ex art. 5 D.L. 14/2017 conv. L. 48/2017 (prevenzione criminalità diffusa/predatoria su pubblica via)	GDPR + D.Lgs. 101/2018	Obbligatoria quando ricorrono i presupposti di rischio elevato; nella prassi, normalmente necessaria in caso di monitoraggio sistematico di spazi pubblici.	Obbligatoria solo in presenza di rischio residuo elevato non mitigabile (art. 36 GDPR).	Come sopra + Patto per la sicurezza urbana Prefetto-Sindaco o altro titolo istituzionale idoneo; documentazione di coordinamento con autorità competenti.
Funzioni di polizia giudiziaria (documentazione di reati, sopralluoghi su notizia di reato, attività sotto direzione dell'Autorità giudiziaria)	D.Lgs. 51/2018 (attuazione Dir. UE 2016/680)	Obbligatoria quando il trattamento presenta un rischio elevato (art. 23 D.Lgs. 51/2018). L'uso di UAS con riprese sistematiche in ambito investigativo rientra normalmente tra i trattamenti a rischio elevato.	Obbligatoria solo se la valutazione di impatto evidenzia un rischio elevato residuo non mitigabile (art. 24 D.Lgs. 51/2018).	Valutazione di impatto; separazione logica e organizzativa degli archivi rispetto ai trattamenti GDPR; registro attività; catena di custodia; verbale di trasmissione all'Autorità giudiziaria.
Funzioni ausiliarie di pubblica sicurezza su richiesta motivata del Prefetto/Questore ex artt. 3 e 5 L. 65/1986	D.Lgs. 51/2018 se la missione è svolta per finalità di prevenzione/contrasto reati o ordine pubblico. Formalizzare per iscritto ruoli e responsabilità tra autorità richiedente e Comando (finalità, istruzioni, accessi, conservazione, sicurezza)	Obbligatoria quando il trattamento presenta rischio elevato (art. 23 D.Lgs. 51/2018).	Obbligatoria solo se permane rischio elevato residuo non mitigabile (art. 24 D.Lgs. 51/2018).	Valutazione di impatto; atto formale di richiesta dell'autorità di PS; disposizione del Sindaco; eventuale accordo scritto che disciplini ruoli e responsabilità; separazione archivi; log accessi.
Volo con finalità mista (componenti amministrative e di polizia giudiziaria nello stesso contesto operativo)	Applicazione distinta dei due regimi, in relazione alla specifica finalità perseguita per ciascun trattamento.	DPIA distinta per ciascun regime oppure unica valutazione con sezioni chiaramente separate, purché siano distinguibili finalità, basi giuridiche, categorie di dati e tempi di conservazione.	Per la componente soggetta a D.Lgs. 51/2018, eventuale consultazione preventiva solo se rischio residuo elevato non mitigabile; per la componente GDPR, art. 36 GDPR.	Separazione effettiva (logica e organizzativa) degli archivi; tracciabilità degli accessi; distinzione dei tempi di conservazione; verbali operativi che identifichino la finalità concreta del volo.

3.1 La DPIA: quando è obbligatoria

La Valutazione d'Impatto sulla Protezione dei Dati (DPIA) è il principale adempimento GDPR che la Polizia Locale deve compiere prima di qualsiasi utilizzo di droni dotati di telecamere o sensori.

Ai sensi dell'art. 35, par. 3, lett. c) GDPR, la DPIA è OBBLIGATORIA per il "monitoraggio sistematico su larga scala di una zona accessibile al pubblico". Le Linee Guida EDPB 3/2019 chiariscono che la videosorveglianza con droni rientra in questa categoria quando è sistematica. Il Garante italiano (Delibera n. 467/2018, docweb 9058979, G.U. n. 269 del 19 novembre 2018) ha pubblicato l'elenco tassativo delle tipologie di trattamento soggette a DPIA obbligatoria: di seguito le categorie specificamente rilevanti per i droni della Polizia Locale.

Garante Privacy, Delibera n. 467 dell'11 ottobre 2018 -- Elenco trattamenti soggetti a DPIA (docweb 9058979, G.U. n. 269/2018)

La Delibera individua le tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre obbligatoriamente a DPIA. Per i droni della Polizia Locale, sono direttamente rilevanti le seguenti categorie dell'Allegato 1: (1) Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati -- vi rientra qualsiasi volo ricorrente o programmato su aree abitate, con o senza registrazione; (2) Trattamenti di categorie particolari di dati (art. 9 GDPR) oppure di dati relativi a condanne penali e reati (art. 10 GDPR) interconnessi con altri dati -- rilevante quando i voli supportano l'accertamento di illeciti penali e i dati sono incrociati con banche dati della Polizia Locale; (3) Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche sistemi di videosorveglianza e geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti -- rilevante se il drone sorvola cantieri, sedi comunali o aree in cui operano lavoratori; (4) Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani) -- rilevante in operazioni di ricerca dispersi o monitoraggio aree frequentate da minori; (5) Trattamenti che comportano la raccolta di dati attraverso reti effettuati anche on-line o attraverso app -- rilevante se il flusso video del drone è trasmesso e registrato via rete (streaming alla centrale operativa). NOTA OPERATIVA: L'elenco non è esaustivo. Il Garante precisa che restano fermi gli obblighi di DPIA nei casi previsti dall'art. 35, par. 3, GDPR e ogni volta in cui ricorrano due o più dei criteri del WP248 rev. 01. Per i droni della Polizia Locale, nella pratica, almeno due criteri dell'elenco ricorrono quasi sempre: uso di nuove tecnologie + monitoraggio di aree pubbliche.

Garante Privacy, Provvedimento n. 10198694 (Comune di Orte) -- NUOVO

Il Garante ha contestato e sanzionato il Comune di Orte per: (1) DPIA mancante ex art. 35 GDPR nonostante il trattamento fosse ad alto rischio; (2) periodo di conservazione dei dati non conforme al principio di limitazione della conservazione ex art. 5, par. 1, lett. e) GDPR. Questo precedente, distinto dal caso Treviso, conferma in modo inequivocabile che la DPIA e la retention policy non sono adempimenti accessori o burocratici, ma condizioni di liceità del trattamento la cui assenza è oggetto di sanzione.

Quando la DPIA è obbligatoria:

- Qualsiasi uso con telecamera che configura un monitoraggio sistematico o ricorrente di persone fisiche identificabili in aree pubbliche o accessibili al pubblico
- Uso di telecamere termiche con capacità identificativa sufficiente a consentire il riconoscimento diretto o indiretto dei soggetti ripresi, o quando le immagini termiche siano utilizzate per selezionare soggetti da sottoporre a controllo (nel caso Treviso il Garante ha archiviato il procedimento proprio perché le sagome erano indistinguibili e non consentivano identificazione; ha tuttavia affermato che la qualificazione dipende dalla funzione e dal contesto, non dalla mera tecnologia impiegata)
- Monitoraggio sistematico o ripetuto di aree pubbliche o private accessibili al pubblico
- Trattamento dati a fini di prevenzione/accertamento illeciti penali (D.Lgs. 51/2018): la DPIA è sempre obbligatoria internamente ai sensi dell'art. 35 D.Lgs. 51/2018; l'invio preventivo al Garante (consultazione preventiva ex art. 36 D.Lgs. 51/2018) è invece dovuto solo in presenza di rischio residuo elevato non mitigabile.

Quando la DPIA è consigliata anche se non strettamente obbligatoria:

- Rilievi aerofotogrammetrici in aree abitate che non configurano monitoraggio sistematico (es. singolo sopralluogo tecnico su un immobile specifico): la DPIA è raccomandata per via della potenziale ripresa incidentale di persone nelle aree circostanti, ma non è formalmente obbligatoria in assenza dei presupposti di sistematicità ex art. 35 GDPR e Delibera Garante 467/2018
- Qualsiasi volo in Categoria Specifica, in ragione della complessità operativa e della maggiore capacità dei sensori tipicamente impiegati, che aumentano la probabilità che ricorrano i presupposti di sistematicità o alto rischio privacy ex art. 35 GDPR (la Categoria Specifica è una classificazione aeronautica, non privacy: il rischio operativo elevato non implica automaticamente obbligo di DPIA, ma ne rende altamente probabile la ricorrenza)
- Primo utilizzo di una nuova tecnologia di sensori

3.2 Privacy by design obbligatorio: il Reg. 2018/1139 Allegato IX

Un elemento che rafforza significativamente l'obbligo di

DPIA e di privacy by design per i droni della Polizia Locale viene direttamente dal regolamento aeronautico europeo, non dal GDPR.

Reg. (UE) 2018/1139, Allegato IX (Requisiti essenziali UAS), punto 1.3

Il legislatore europeo ha inserito direttamente nei requisiti essenziali degli UAS l'obbligo di incorporare la privacy fin dalla progettazione: "Se necessario al fine di attenuare i rischi inerenti alla sicurezza, alla tutela della riservatezza, alla protezione dei dati personali, alla security o all'ambiente derivanti dal loro esercizio, gli aeromobili senza equipaggio devono possedere le relative caratteristiche e funzionalità specifiche che tengono conto dei principi della tutela della riservatezza e della protezione dei dati personali fin dalla progettazione e per impostazione predefinita". Allegato IX, punto 1.1: operatori e piloti remoti devono "essere a conoscenza delle norme nazionali e dell'Unione applicabili alle operazioni previste, in particolare in materia di sicurezza, tutela della riservatezza, protezione dei dati, responsabilità civile, assicurazione, security e protezione dell'ambiente".

IMPLICAZIONE OPERATIVA: il privacy by design per i droni non è un adempimento aggiuntivo ricavato per analogia dal GDPR, ma un obbligo strutturale del regolamento aeronautico europeo (Allegato IX Reg. 2018/1139), vincolante per il costruttore e per l'operatore. Ne derivano tre conseguenze concrete: (a) il Comandante di Polizia Locale deve verificare, in fase di acquisto del drone, che il costruttore abbia implementato le funzionalità di privacy by design (richiesta di documentazione tecnica e dichiarazione di conformità all'Allegato IX); (b) l'obbligo di DPIA si estende a qualsiasi uso con sensori che possano riprendere persone, a prescindere dalla Categoria ENAC; (c) le misure di protezione dati (anonimizzazione, minimizzazione, geo-fencing, crittografia del flusso) non sono optional ma parte del "design obbligatorio" dell'aeromobile.

3.3 La questione del drone "termico" e dell'identificabilità

Il punto non è solo "vedo il volto". Il Garante, nel caso Treviso, ha affermato espressamente che l'impiego di droni con termocamere per generare mappe di calore, sulla base delle quali si indirizzano controlli sul territorio, può comportare trattamento di dati personali, anche relativi a reati. Questo sposta l'analisi dall'hardware alla funzione e al contesto: anche sagome termiche indistinguibili singolarmente possono essere dati personali se, in quel contesto, consentono l'identificazione indiretta o la selezione di soggetti da sottoporre a controllo.

3.4 Il D.P.R. 15 gennaio 2018, n. 15: la disciplina speciale per le Forze di polizia

Il D.P.R. 15 gennaio 2018, n. 15 (G.U. n. 61 del 14 marzo 2018, in vigore dal 29 marzo 2018) disciplina il trattamento dei dati personali effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia ex art. 57 D.Lgs. 196/2003. AVVERTENZA FONDAMENTALE: come accertato sul testo della norma primaria, l'art. 1, comma 3 esclude espressamente la Polizia Locale dal suo ambito applicativo diretto. Il D.P.R. rileva per la Polizia Locale unicamente come parametro interpretativo e standard di buona prassi.

D.P.R. 15 gennaio 2018, n. 15 -- artt. 1 c. 3, 6, 22, 23 cc. 3-4 e 24 (G.U. n. 61/2018)

Art. 1, c. 3: "il presente regolamento non si applica ai soggetti pubblici che, pur effettuando il trattamento dei dati personali per le finalità di polizia di cui all'articolo 3, non rientrano nella categoria degli organi, uffici e comandi di cui all'articolo 57 del Codice" -- esclude direttamente la Polizia Locale. Art. 23, c. 3: "il trattamento di dati personali raccolti tramite aeromobili a pilotaggio remoto, in considerazione della loro potenziale invasività, è ricompreso tra quelli che presentano rischi specifici di cui all'articolo 6". Art. 23, c. 4: "l'utilizzo di sistemi di ripresa fotografica, video e audio, installati su aeromobili a pilotaggio remoto, è autorizzato al livello gerarchico non inferiore a quello di capo ufficio o comandante di reparto". Artt. 6, c. 2 e 24, c. 4 (nota: alcune fonti secondarie attribuivano erroneamente questo obbligo all'art. 23 -- la verifica sul testo primario ha accertato la corretta collocazione): obbligo di file di log non modificabili, conservati per cinque anni dall'accesso o dall'operazione, accessibili ai soli fini della verifica della liceità del trattamento, del controllo interno e nell'ambito del procedimento penale.

⚠ ATTENZIONE

AMBITO DI APPLICAZIONE -- AVVERTENZA PRELIMINARE INDISPENSABILE: L'art. 1, comma 3 del D.P.R. 15/2018 stabilisce espressamente che "il presente regolamento non si applica ai soggetti pubblici che, pur effettuando il trattamento dei dati personali per le finalità di polizia di cui all'articolo 3, non rientrano nella categoria degli organi, uffici e comandi di cui all'articolo 57 del Codice [D.Lgs. 196/2003]". La Polizia Locale NON è ricompresa tra gli organi ex art. 57 D.Lgs. 196/2003, che si riferisce esclusivamente alle Forze di polizia ex art. 16 L. 121/1981. Il D.P.R. 15/2018 NON è quindi applicabile direttamente alla Polizia Locale. Il richiamo alla norma è legittimo esclusivamente come parametro interpretativo e standard di buona prassi, non come fonte vincolante.

Fatta questa premessa indispensabile, il D.P.R. 15/2018 conserva per la Polizia Locale una rilevanza interpretativa significativa su tre profili specifici, verificati direttamente sul testo della norma primaria (G.U. n. 61 del 14 marzo 2018):

- **Art. 23, c. 3** -- Riconoscimento legislativo della specificità del drone: la norma classifica il trattamento dati via APR tra quelli che "presentano rischi specifici di cui all'articolo 6", in considerazione della loro "potenziale invasività". Questo riconoscimento proveniente dal legislatore nazionale rafforza l'argomento per cui anche la Polizia Locale -- soggetta al GDPR e al D.Lgs.

51/2018 -- è tenuta ad applicare misure più stringenti rispetto alla videosorveglianza fissa, indipendentemente dalla categoria operativa ENAC (open, specific, certified). *Ne deriva che la DPIA ex art. 35 GDPR è da considerarsi, nella sostanza, obbligatoria per qualsiasi uso di droni dotati di sensori, anche in Category Open — fatte salve le eccezioni per voli sporadici non sistematici descritte al cap. 3.1.*.

- **Art. 23, c. 4** -- Standard gerarchico di autorizzazione: la norma prevede che l'utilizzo di sistemi di ripresa installati su APR sia "autorizzato al livello gerarchico non inferiore a quello di capo ufficio o comandante di reparto". Pur non vincolando direttamente la Polizia Locale, questo requisito costituisce il riferimento pratico più specifico disponibile nell'ordinamento per la catena autorizzativa interna: il regolamento interno della Polizia Locale dovrebbe prevedere che ogni missione drone dotata di sensori sia autorizzata almeno dal Comandante di Polizia Locale o da un ufficiale formalmente delegato, con atto scritto e tracciato.
- **Artt. 6, c. 2 e 24, c. 4** -- Standard tecnici per i file di log: gli accessi e le operazioni sui dati raccolti via drone devono essere "registrati in appositi file di log, non modificabili, che sono conservati per cinque anni dall'accesso o dall'operazione". Questi standard tecnici -- non specificati con analogo dettaglio né nel GDPR né nel D.Lgs. 51/2018 -- costituiscono il riferimento più preciso disponibile nell'ordinamento nazionale per la gestione dei log nelle riprese via drone e vanno recepiti nel regolamento interno della Polizia Locale come misura tecnica minima di sicurezza.

⚠ ATTENZIONE

LACUNA NORMATIVA CONFERMATA: Il testo del D.P.R. 15/2018 (G.U. n. 61/2018) conferma che nessuna norma regolamentare nazionale disciplina direttamente il trattamento dati via APR da parte della Polizia Locale. Il D.P.R. 15/2018 si applica esclusivamente alle Forze di polizia ex art. 57 D.Lgs. 196/2003; il DM 13.06.2022 disciplina solo le modalità operative delle Forze di polizia ex art. 16 L. 121/1981. Per la Polizia Locale, il quadro è costruito per analogia da GDPR, D.Lgs. 51/2018 e dai suddetti atti come parametri di buona prassi. Questa lacuna rende indispensabile il regolamento interno e la DPIA come unici strumenti di garanzia sostituivi della norma speciale assente.

3.5 Caso Pescara (body cam Polizia Locale): parere negativo del Garante e riflessi sui droni

Con provvedimento n. 743 del 4 dicembre 2025 (docweb 10221993, G.U. consultabile su garanteprivacy.it), il Garante per la protezione dei dati personali ha espresso parere NON FAVOREVOLE sulla DPIA presentata dal Comune di Pescara relativa all'uso di body cam da parte della Polizia Locale. Si trattava della quarta versione della DPIA, presentata dopo reiterati cicli di interlocuzione con il Garante a partire dal 2022. Il provvedimento contiene affermazioni di principio rilevanti anche per i droni.

Principi desumibili dal Provv. n. 743/2025 rilevanti per i droni Polizia Locale

1. D.P.R. 15/2018 NON applicabile alla Polizia Locale (conferma esplicita): Il Garante ha ribadito che "gli organi della Polizia municipale sono esclusi dall'applicazione del D.P.R. 15/2018" (art. 1, c. 3 del regolamento). Questo conferma la tesi già sostenuta nel cap. 3.4: il D.P.R. 15/2018 è applicabile solo per via interpretativa/analogica, non direttamente.

2. Cloud provider extra-UE = rischio sistemico: Il Tra i profili critici rilevati dal Garante figura la circostanza che il sistema di gestione dati fosse riferibile a un'azienda statunitense: il provvedimento segnala questo elemento come criticità non adeguatamente chiarita sul piano della conformità alla Direttiva 2016/680, senza che il Comune avesse fornito sufficienti garanzie tecniche e giuridiche al riguardo. Lo stesso rischio si pone per i droni che caricano filmati su cloud (es. DJI FlightHub, piattaforme non UE): il Comune deve verificare la localizzazione dei server e imporre contrattualmente l'archiviazione in UE.

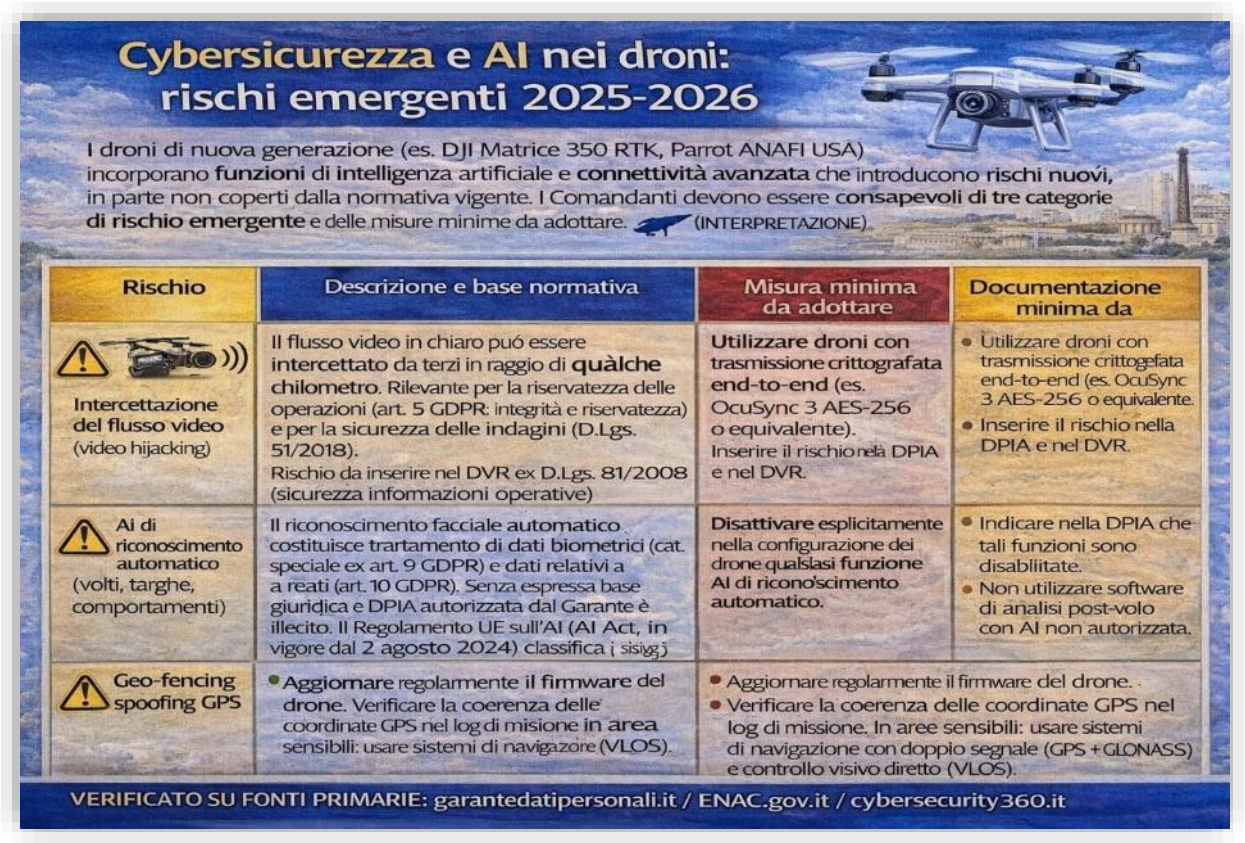
3. La DPIA è un processo iterativo, non un adempimento una tantum: Pescara ha presentato quattro versioni in tre anni. Il Garante ha richiesto in ciascuna versione ulteriori approfondimenti tecnici. La DPIA per droni deve essere redatta con adeguata competenza tecnica (non solo giuridica) e deve rispondere puntualmente alle osservazioni del Garante se quest'ultimo viene coinvolto preventivamente.

IMPLICAZIONE OPERATIVA: I Comandi che stanno valutando l'acquisto di droni con funzioni di streaming o archiviazione cloud devono: (a) verificare la localizzazione dei server del fornitore; (b) verificare e documentare contrattualmente le modalità di accesso del fornitore ai dati, aspetto che il Garante ha indicato come insufficientemente chiarito nel caso Pescara; (c) preferire soluzioni con archiviazione on-premise o su cloud certificato UE (es. GAIA-X compliant). La stessa verifica vale per la piattaforma di gestione del volo (es. DJI AeroScope, FlightHub).

3.6 Cybersicurezza e AI nei droni: rischi emergenti 2025-2026

I droni di nuova generazione (es. DJI Matrice 350 RTK, Parrot ANAFI USA) incorporano funzioni di intelligenza artificiale e connettività avanzata che introducono rischi nuovi, in parte non coperti dalla normativa vigente. I Comandanti devono essere consapevoli di tre categorie di rischio emergente e delle misure minime da adottare.

Rischio	Descrizione e base normativa	Misura minima da adottare
Intercettazione del flusso video (video hijacking)	Il flusso video in chiaro può essere intercettato da terzi in raggio di qualche chilometro. Rilevante per la riservatezza delle operazioni (art. 5 GDPR: integrità e riservatezza) e per la sicurezza delle indagini (D.Lgs. 51/2018). Rischio da inserire nel DVR ex D.Lgs. 81/2008 (sicurezza informazioni operative).	Utilizzare droni con trasmissione crittografata end-to-end (es. OcuSync 3 AES-256 o equivalente). Inserire il rischio nella DPIA e nel DVR.
AI di riconoscimento automatico (volti, targhe, comportamenti)	Il riconoscimento facciale automatico costituisce trattamento di dati biometrici (cat. speciale ex art. 9 GDPR) e dati relativi a reati (art. 10 GDPR). Senza espressa base giuridica e DPIA autorizzata dal Garante è illecito. Il Reg. (UE) 2024/1689 (AI Act, in vigore dal 1° agosto 2024, con regime transitorio per le diverse categorie) pone limiti molto stringenti all'uso di sistemi di identificazione biometrica remota, con un regime particolarmente restrittivo per le autorità di contrasto che va oltre la semplice classificazione come "alto rischio". Prima di qualunque uso operativo di funzioni di riconoscimento biometrico, è indispensabile una verifica specifica del perimetro normativo applicabile, inclusi i vincoli del D.Lgs. 51/2018 e le eventuali autorizzazioni richieste.	Disattivare esplicitamente nella configurazione del drone qualsiasi funzione AI di riconoscimento automatico. Indicare nella DPIA che tali funzioni sono disabilitate. Non utilizzare software di analisi post-volo con AI non autorizzata.
Geo-fencing e spoofing GPS	Il geo-fencing del drone può essere aggirato tramite spoofing GPS, con rischio di ingresso in zone vietate (aeroporti, infrastrutture critiche). La responsabilità del Comandante è integra anche in caso di malfunzionamento tecnologico se non sono state adottate le cautele del caso (D.Lgs. 81/2008, art. 17).	Aggiornare regolarmente il firmware del drone. Verificare la coerenza delle coordinate GPS nel log di missione. In aree sensibili: usare sistemi di navigazione con doppio segnale (GPS + GLONASS) e controllo visivo diretto (VLOS).



3.7 Sistemi integrati Polizia Locale/Forze di polizia: contitolarità o titolarità distinta?

Un tema di rilievo pratico riguarda i casi in cui il sistema di videosorveglianza (o il flusso video di un drone) gestito dalla Polizia Locale è reso accessibile anche alle Forze di polizia dello Stato (Questura, Carabinieri, ecc.) nell'ambito di protocolli di sicurezza integrata. La questione è se questa condivisione tecnica configuri una **contitolarità del trattamento** ex art. 26 GDPR oppure due distinte e autonome titolarità. La risposta ha conseguenze concrete sulla governance del trattamento, sulle responsabilità e sugli obblighi di informativa verso i cittadini.

Principio: titolarità distinte e parallele, non contitolarità

L'art. 26 GDPR prevede la contitolarità quando due o più titolari determinano «congiuntamente le finalità e i mezzi del trattamento». L'EDPB (ex WP29) precisa che questo presuppone un trattamento «inseparabile» o «indissolubilmente legato» tra le parti: se il trattamento di ciascuno non sarebbe possibile senza la partecipazione dell'altra, allora vi è contitolarità. Nel caso dei sistemi di videosorveglianza comunale condivisi con le Forze di polizia, la situazione è invece quella di **autonome titolarità distinte e parallele**: il Comune persegue finalità di sicurezza urbana e polizia amministrativa locale; la Questura/Prefettura persegue finalità di pubblica sicurezza e ordine pubblico. Le finalità sono giuridicamente distinte (corrispondenti alla distinzione sicurezza primaria/secondaria di cui alla sez. 1.3-bis) e nessun soggetto può determinare unilateralmente le finalità dell'altro. La condivisione tecnica del flusso video non modifica questa struttura. [Fonte: Vademecum videosorveglianza Comuni e Unioni di Comuni, Lepida/Regione Emilia-Romagna, feb. 2022, App. A; conforme a EDPB Guidelines 3/2019 e art. 26 GDPR]

Conseguenze pratiche della titolarità distinta:

1. Il Comune tratta le immagini esclusivamente per le proprie finalità istituzionali (sicurezza urbana, polizia amministrativa locale): non può conferire alle Forze di polizia accesso illimitato né finalità di utilizzo diverse da quelle dichiarate nella propria DPIA.
2. Le Forze di polizia che accedono al sistema (Questura, Carabinieri, ecc.) sono titolari autonomi per i trattamenti che effettuano con quelle immagini ai fini di pubblica sicurezza/ordine pubblico: il loro trattamento rientra nel D.Lgs. 51/2018 (Direttiva 2016/680), non nel GDPR.
3. Il soggetto che gestisce tecnicamente il sistema condiviso (es. società in-house, provider ICT) deve essere nominato **responsabile del trattamento ex art. 28 GDPR** da ciascun titolare separatamente. Non è sufficiente un unico contratto di servizio generico: ciascun titolare deve avere il proprio atto di nomina del responsabile, con specifici obblighi, finalità e misure di sicurezza.
4. I profili di accesso al sistema devono essere configurati in modo da separare le finalità: il personale della Questura deve poter accedere solo alle immagini/sequenze per cui ha titolo (es. su richiesta formale ai sensi dell'art. 3 L. 65/1986), non all'intero archivio del sistema comunale. L'accesso indiscriminato delle Forze di polizia al sistema comunale è incompatibile con il principio di limitazione delle finalità ex art. 5(1)(b) GDPR e con la struttura della titolarità distinta.

⚠ ATTENZIONE — Errore frequente: l'accordo di «sicurezza integrata» non crea contitolarità

Il Patto per la sicurezza urbana (art. 5 D.L. 14/2017) o il protocollo tecnico di interconnessione dei sistemi di videosorveglianza non costituiscono di per sé un «accordo di contitolarità» ex art. 26 GDPR. Configurare giuridicamente la relazione Polizia Locale/Forze di polizia come contitolarità è un errore che produce conseguenze gravi: (a) implicherebbe che il Comune co-determina le finalità di sicurezza primaria delle Forze di polizia, sconfinando in una competenza che il quadro costituzionale (artt. 117 co. 2 lett. h) Cost.; C. Cost. n. 285/2019) riserva allo Stato; (b) esporrebbe il Comune a responsabilità per trattamenti di dati (D.Lgs. 51/2018) che non gli competono; (c) renderebbe necessario un accordo formale che definisca le responsabilità ex art. 26(1) GDPR, con obblighi di pubblicazione verso gli interessati, applicabile solo se davvero vi è determinazione congiunta. La soluzione corretta è: mantenere titolarità distinte, con accesso delle Forze di polizia ai sistemi comunali disciplinato da protocollo formale limitato alle finalità autorizzate (art. 3 L. 65/1986), e gestore tecnico condiviso nominato responsabile ex art. 28 GDPR da ciascun titolare separatamente. Il Comitato provinciale per l'ordine e la sicurezza pubblica (art. 20 L. 121/1981) e il Comitato metropolitano (art. 6 D.L. 14/2017) sono le sedi istituzionali appropriate per condividere specifiche e finalità dei sistemi, non per costituire contitolarità del trattamento.

3.8 Trasparenza e informativa con i droni (art. 13-14 GDPR)

Con i droni, la segnaletica fisica tipo "zona videosorvegliata" può essere insufficiente o materialmente inidonea (il drone si sposta). L'EDPB, nelle Linee Guida 3/2019, insiste su un'informativa stratificata: informativa breve in prossimità dell'area operativa (con QR code per quella estesa) e informativa completa su pagina web istituzionale. Se il trattamento rientra nel D.Lgs. 51/2018 (finalità di law enforcement), le regole sull'informativa seguono quel quadro, che prevede limitazioni all'obbligo di informativa ma requisiti stringenti di tracciamento e separazione degli archivi.

3.9 Principi fondamentali da rispettare

- Minimizzazione dei dati: raccogliere solo i dati strettamente necessari alla finalità. Configurare il drone con angoli, zoom e aree di ripresa limitati. Preferire volo senza registrazione quando non strettamente necessaria.
- Limitazione della finalità: i dati raccolti con il drone NON possono essere riutilizzati per finalità diverse da quelle indicate nella DPIA.
- Limitazione della conservazione (retention policy): definire i tempi di cancellazione e rispettarli. Il caso Orte dimostra che la mancanza di retention policy è sanzionata.
- Integrità e riservatezza: cifratura dei file, accesso limitato al personale autorizzato, log degli

accessi.
- Separazione degli archivi: distinguere i dati trattati ex GDPR (finalità amministrative) da quelli trattati ex D.Lgs. 51/2018 (finalità di PG/law enforcement).
- Accountability: tenere un registro delle missioni come prova del rispetto di tutti i principi (art. 5, par. 2 GDPR).

4. Utilizzabilità probatoria delle riprese: profilo processuale e penale

Il drone della Polizia Locale, quando effettua riprese video o fotografiche, produce materiale che può essere destinato a uso probatorio in procedimenti penali o in procedimenti sanzionatori amministrativi. È fondamentale che l'operatore conosca in anticipo il regime processuale applicabile, le condizioni di utilizzabilità e i limiti invalicabili, anche perché un'immagine acquisita in violazione di tali limiti non solo è inutilizzabile come prova, ma può configurare un reato.

4.1 Le riprese su luoghi pubblici come prova documentale

L'art. 234 c.p.p. consente l'acquisizione come prova documentale di scritti o altri documenti che rappresentano fatti, persone o cose mediante fotografia, cinematografia, fonografia o qualsiasi altro mezzo. Le riprese effettuate dal drone su luoghi pubblici o aperti al pubblico per documentare fatti (abbandono di rifiuti, dinamica di un sinistro, presenza di una discarica abusiva, abuso edilizio in atto) si collocano tipicamente in questa categoria.

Cass. pen., Sez. IV, sent. n. 21557/2024

Tratta l'utilizzabilità di videoriprese effettuate in luoghi pubblici/aperti al pubblico e affronta l'inquadramento rispetto alle intercettazioni e ai mezzi di ricerca della prova. La decisione conferma l'orientamento secondo cui la videoripresa in luoghi pubblici può essere utilizzata come acquisizione documentale/prova (art. 234 c.p.p.) senza automatica assimilazione alle intercettazioni, con le dovute cautele. Implicazione pratica: le riprese drone su aree pubbliche per documentare fatti (dinamica incidente, abbandono rifiuti) tendono a collocarsi sul versante documentale e sono tendenzialmente ammissibili come prova.

Per l'art. 189 c.p.p. (prove non disciplinate dalla legge), il giudice può ammettere prove atipiche se idonee all'accertamento e non lesive della libertà morale. È il riferimento normativo sussidiario per alcune videoriprese. In entrambi i casi, la robustezza probatoria dipende in modo critico da: integrità del file (hash), catena di custodia documentata, log di accesso, assenza di manipolazione.

4.2 I limiti invalicabili: art. 615-bis c.p. e spazi di vita privata

⚠ ATTENZIONE

LIMITE ASSOLUTO: Il drone NON deve MAI essere progettato per captare stabilmente l'interno di abitazioni o spazi di vita privata (luoghi ex art. 614 c.p.). Chi lo fa commette il reato di "interferenze illecite nella vita privata" ex art. 615-bis c.p. (reclusione da 6 mesi a 4 anni, aggravata per pubblici ufficiali che agiscono con abuso dei poteri). Le immagini così acquisite sono inutilizzabili come prova. Se emergono esigenze investigative che richiedono la captazione di ambienti privati, vanno attivati i canali di polizia giudiziaria sotto direzione dell'Autorità Giudiziaria e con gli strumenti processuali appropriati (intercettazioni, ispezioni con decreto motivato).

La "red line" operativa va fissata nei protocolli interni in modo chiaro: le operazioni drone non devono essere progettate per captare l'interno di abitazioni, cortili privati, o altri spazi di vita privata. Il fatto che il sorvolo avvenga ad alta quota non è di per sé sufficiente a escludere la violazione se le ottiche del drone sono in grado di acquisire immagini di qualità tale da penetrare la sfera privata.

4.3 Alert per uso in contesti lavorativi

Il rischio del controllo a distanza dei lavoratori si concretizza ogni volta che il drone della Polizia Locale sorvola aree in cui sono presenti lavoratori in attività: cantieri comunali o privati, magazzini e depositi aziendali, mercati rionali con operatori, aree portuali o industriali. In questi contesti, se le riprese consentono di documentare l'attività lavorativa di soggetti identificabili, si applica la tutela dell'art. 4 della Legge 300/1970 (Statuto dei Lavoratori), che vieta il controllo a distanza dei lavoratori senza accordo sindacale o autorizzazione dell'Ispettorato del Lavoro. L'uso del drone in tali situazioni deve essere espressamente disciplinato nel regolamento interno e nella DPIA, con esplicita esclusione delle finalità di controllo dell'attività lavorativa.

Cass. pen., Sez. III, sent. n. 50919/2019 (videosorveglianza lavorativa)

Conferma la rilevanza penale della videosorveglianza in violazione delle garanzie sui controlli a distanza (art. 4 L. 300/1970 -- Statuto dei Lavoratori). Sebbene non sia un caso drone, è un precedente rilevante perché un drone impiegato per controllare accessi o attività di lavoratori comunali (cantieri, dipendenti impegnati in servizio esterno, operatori di aziende partecipate) potrebbe creare lo stesso problema giuridico. Implicazione: il regolamento interno sull'uso dei droni deve vietare espressamente l'uso per monitorare l'attività dei lavoratori; la formazione dei piloti deve includere questo scenario.

4.4 La catena di custodia: requisiti pratici

Per garantire l'utilizzabilità processuale delle immagini, il protocollo operativo deve prevedere le seguenti misure minime:

- Calcolo dell'hash del file al momento dello scarico dal drone (hash SHA-256 o equivalente), da registrare nel log di missione
- Conservazione del file originale in formato non modificabile (read-only) con accesso limitato e tracciato
- Log di tutti gli accessi al file (chi, quando, perché), con firma del responsabile
- Verbale di acquisizione che documenta: missione, data/ora/luogo, pilota, drone, hash, copia del log di volo
- In caso di trasferimento all'AG o alle Forze di polizia: verbale di consegna con hash del file ricevuto e firma del destinatario
- Divieto assoluto di editing o post-processing del file originale; se necessarie copie di lavoro, queste devono essere chiaramente identificate come tali

5. Procedure operative

La tabella seguente presenta in modo schematico tutte le procedure da adottare, organizzate per fase.

Fase	Adempimento	Riferimento normativo / Note operative
PRE-OPERATIVA	1. Delibera/determinazione amministrativa che individua le finalità d'uso e ne giustifica la necessità rispetto ad alternative meno invasive (principio di proporzionalità)	Base giuridica art. 6, par. 1, lett. e) GDPR. Necessaria per giustificare il trattamento dati
PRE-OPERATIVA	2. Se finalità di “sicurezza urbana” (prevenzione criminalità diffusa/predatoria): stipula del Patto per la sicurezza urbana tra Prefetto e Sindaco ex art. 5 D.L. 14/2017, o acquisizione della richiesta formale scritta del Prefetto/Questore + disposizione del Sindaco ex artt. 3 e 5, co. 1, lett. c) L. 65/1986, per le specifiche operazioni di PS ausiliarie (ATTENZIONE: non è una “delega” in senso tecnico ma una “richiesta motivata” che attiva il meccanismo ausiliario)	D.L. 14/2017 conv. L. 48/2017, art. 5; L. 65/1986, artt. 3 e 5, co. 1, lett. c) e co. 4; Garante Provv. n. 10013356/2024: non basta delibera interna del Comune; Ministero dell’Interno, Gabinetto del Ministro, Ufficio II – Ordine e Sicurezza Pubblica, circolare prot. 11001/123/111 (3), prot. uscita n. 0031004 del 7 aprile 2025, recante indicazioni applicative sui Patti per l’attuazione della sicurezza urbana e l’installazione di sistemi di videosorveglianza
PRE-OPERATIVA	3. Acquisto UAS conforme alle classi CE (C0-C4 per Open; C5-C6 per STS-EASA)	Reg. UE 2019/945; Reg. UAS-IT ENAC 2021
PRE-OPERATIVA	4. Registrazione del Comune (in qualità di Operatore UAS) sul portale D-Flight e acquisizione QR code identificativo. NOTA: l'obbligo di immatricolazione si applica a qualsiasi UAS dotato di sensori in grado di raccogliere dati personali (es. videocamera), a prescindere dal peso (art. 14 Reg. 2019/947, Considerando 8) -- anche i mini-droni < 250 g con fotocamera richiedono immatricolazione dell'operatore se dotati di videocamera	Art. 6 e 9 Reg. UAS-IT ENAC; art. 14 Reg. UE 2019/947; Considerando 8 Reg. 2019/947
PRE-OPERATIVA	5. Formazione e conseguimento attestato pilota: A1/A3 (Open) o A2 (Open A2) o corsi aggiuntivi SORA/CRM (Specific); per UAS >= 25 kg, titolo aeronautico e qualificazione CEA-APR Aeronautica Militare. IMPORTANTE: l'esame teorico A1/A3 include obbligatoriamente la materia “riservatezza e protezione dei dati” tra le 40 domande (UAS.OPEN.020 par. 5 Reg. 2019/947) -- il pilota certificato ha per definizione superato un test su privacy, non è facoltativo	Reg. UE 2019/947; Reg. UAS-IT ENAC; D.M. Interno 13.06.2022 art. 7, co. 2 (per UAS >= 25 kg). La formazione deve includere anche scenari “sensibili” (assembramenti, aree private, strutture critiche, contesti lavorativi)
PRE-OPERATIVA	5b. D.Lgs. 81/2008 (Testo Unico Sicurezza Lavoro) -- ADEMPIMENTO AUTONOMO: il Comune in quanto datore di lavoro pubblico deve includere nel DVR del Comando l’attività con UAS come mansione a sé stante (rischi specifici: stanchezza visiva prolungata, esposizione a condizioni meteorologiche avverse, gestione emergenze a terra, stress da concentrazione); formazione specifica del pilota-dipendente sui rischi della mansione; verificare l’idoneità sanitaria se richiesta. NOTA: questo obbligo riguarda esclusivamente la tutela del LAVORATORE-PILOTA, ed è del tutto autonomo rispetto agli adempimenti GDPR, aeronautici e di sicurezza pubblica	D.Lgs. 9 apr. 2008, n. 81 (TUSL), artt. 17 co. 1 lett. a) (DVR non delegabile), 28 (contenuto DVR), 36-37 (informazione e formazione lavoratori); si applica a tutti i settori pubblici e privati senza eccezioni
PRE-OPERATIVA	6. Stipula polizza assicurativa RC per responsabilità verso terzi (massimale minimo 750.000 DSP ~ EUR 913.000)	Art. 27 Reg. UAS-IT ENAC; Reg. CE 785/2004
PRE-OPERATIVA	7. Conduzione della DPIA; per trattamenti a fini di prevenzione/accertamento reati (D.Lgs. 51/2018): invio preventivo al Garante solo in presenza di rischio residuo elevato non mitigabile.	Art. 35 GDPR; D.Lgs. 51/2018; Linee Guida EDPB 3/2019; Garante Delibera 467/2018 (elenco trattamenti soggetti a DPIA, docweb 9058979); Garante Provv. n. 10198694 (Comune di Orte): DPIA mancante e conservazione non conforme sono violazioni sanzionate
PRE-OPERATIVA	8. Adozione del Manuale delle Operazioni (obbligatorio in Categoria Specifica)	Art. UAS.SPEC.030 Reg. UE 2019/947; AMC1 UAS.SPEC.030
PRE-OPERATIVA	9. Adozione di un regolamento interno sull'uso dei droni che disciplini: finalità ammesse, esclusione esplicita del controllo a distanza dei lavoratori, conservazione dati (retention policy), accessi, sicurezza, procedura gestione incidenti e data breach	Art. 32 e 5, par. 2 GDPR (accountability); art. 4 L. 300/1970 (Statuto Lavoratori); Cass. pen. n. 50919/2019: alert per uso in prossimità di strutture con personale

Fase	Adempimento	Riferimento normativo / Note operative
PRE-OPERATIVA	10. Se si intende operare come Volo di Stato (esenzione dalla normativa civile): richiesta di accreditamento ENAC ex art. 71, par. 1 Reg. UE 2018/1139	Art. 2, par. 3, lett. a) Reg. UE 2018/1139; Nota ENAC “esenzione ai sensi art. 71(1)”
PIANIFICAZIONE MISSIONE	11. Verifica delle zone geografiche UAS su D-Flight (Circolare ENAC ATM-09A) e verifica delle zone a divieto/restrizione di volo (Circolare ENAC ATM-03C); identificare aree vietate ex art. 793 Cod. Nav.	Circolare ENAC ATM-09A; Circolare ENAC ATM-03C; D.Lgs. 96/2005 (art. 793 Cod. Nav.); AIP; L. 394/1991 (parchi nazionali). Documentare con screenshot/estratto zona + log di pianificazione
PIANIFICAZIONE MISSIONE	12. Per aree soggette a divieto di sorvolo ex art. 793 Cod. Nav.: acquisire autorizzazione ENAC + nulla osta/assenso del gestore/proprietario del sito + eventuale coordinamento con autorità di PS competente	Art. 793 Cod. Nav. come sost. da D.Lgs. 96/2005; Reg. UAS-IT ENAC (obbligo autorizzazione ENAC); Circolare ATM-03C
PIANIFICAZIONE MISSIONE	13. Eventuale richiesta di riserva di spazio aereo alla Direzione Territoriale ENAC competente (se oltre 120 m, in CTR, o se richiesto dalla SORA)	Allegato B alla Circolare ENAC ATM-09A
OPERATIVA	14. Rispetto dei limiti operativi: VLOS, altitudine max 120 m (Open) o secondo autorizzazione (Specific), distanze di sicurezza dalle persone, divieto di sorvolo di assembramenti in A2/A3	Reg. UE 2019/947, art. UAS.OPEN.020 ss.; Reg. UAS-IT ENAC. Configurare geofencing e briefing piloti; documentare eventuali eccezioni autorizzate
OPERATIVA	15. Apposizione del QR code identificativo sul drone prima del decollo e verifica Remote ID attivo (per UAS C1-C6)	Art. 6 e 9 Reg. UAS-IT ENAC; Reg. UE 2019/945
OPERATIVA	16. Emissione di un ordine di servizio/autorizzazione interna alla missione che indichi: finalità, categoria operativa, zone di volo, limiti operativi (quota, perimetro, durata), regime privacy applicabile (GDPR o D.Lgs. 51/2018), nominativi piloti/operatori, regole su registrazione e conservazione dati, divieto ripresa interni abitazioni, procedura incidente	Reg. UAS-IT ENAC; GDPR artt. 5, 32; Cass. pen. n. 21557/2024: importanza della delimitazione delle riprese e della documentazione dei log
OPERATIVA	17. Registrazione della missione nel log operativo (data, ora, luogo, durata, finalità, pilota, drone, condizioni meteo, eventuali anomalie)	Art. UAS.SPEC.050; buona prassi per Categoria Aperta; necessario per accountability GDPR (art. 5, par. 2)
OPERATIVA - PROVA	18. Se le riprese sono destinate a uso probatorio: garantire integrità del file (hash), catena di custodia documentata, log di accesso, non manipolazione; limitare le riprese a luogo pubblico o aperto al pubblico; escludere tassativamente captazioni dell'interno di abitazioni o spazi di vita privata	Art. 234 c.p.p. (prova documentale); art. 189 c.p.p. (prove atipiche); Cass. pen. Sez. IV n. 21557/2024; art. 615-bis c.p.: riprese di luoghi di privata dimora senza autorizzazione AG = reato + inutilizzabilità della prova
POST-OPERATIVA	19. Conservazione e cancellazione dei dati secondo la retention policy (principi di minimizzazione e limitazione della conservazione)	Art. 5, par. 1, lett. c) ed e) GDPR; D.Lgs. 51/2018; Garante Provv. n. 10198694 (Comune di Orte): conservazione non conforme è violazione sanzionata
POST-OPERATIVA	20. Accesso alle immagini limitato al personale autorizzato; misure di sicurezza tecniche e organizzative (cifratura, log degli accessi, separazione archivi GDPR/D.Lgs. 51/2018)	Art. 32 GDPR; art. 29 D.Lgs. 51/2018; Linee Guida EDPB 3/2019
POST-OPERATIVA	21. In caso di incidente/inconveniente grave: notifica ad ENAC e comunicazione ad ANSV entro 60 minuti; valutare se l'incidente ha coinvolto dati personali (data breach) e, in tal caso, notifica al Garante Privacy entro 72 ore	Reg. UAS-IT ENAC (obbligo occurrence reporting, ANSV entro 60 min.); art. 33 GDPR (data breach entro 72 ore al Garante)
POST-OPERATIVA	22. Audit periodico del sistema (conformità aeronautica, conformità GDPR, verifica retention policy, aggiornamento DPIA se cambia il contesto operativo); considerare il profilo di responsabilità contabile (Corte dei Conti) per acquisti non conformi e spreco di risorse	Art. 5, par. 2 GDPR (accountability); normativa sulla responsabilità amministrativo-contabile; art. 82 GDPR (risarcimento danni da trattamento illecito)


USO DEI DRONI – PROTOCOLLO OPERATIVO
FASI, ADEMPIMENTI E RIFERIMENTI NORMATIVI
FASE
Adempimento
1. Delibera che individua finalità di uso
Art. 6 GDPR
2. Patto per la sicurezza urbana
Art. 5 D.L. 14/2017 • Reg. UE 51/ττες
3. Acquisto UAS conforme classi CE
• Reg. UE 2019/945 • Reg. UE 2019/945
4. Registrazione Operatore del Comune
• Art. 14 Reg. UE 2019/947
5. Attestato pilota A1/A3 o A2
• Reg. UE 2019/947 • Reg. UE 2019/947
PIANIFICAZIONE MISSIONE
6. Verifica zone geografiche UAS
• Circolari ENAC.
7. Autorizzazione sorvolo aree riservate
• Art. 793 Cod. Nav.
8. Eventuale riserva spazio aereo ENAC
• Reg. UE 2019/947
ENAC
OPERATIVA
9. Rispetto limiti operativi: VLOS, max 120m
• Reg. UE 2019/947
10. Apposizione QR code / Remote ID
• Reg. UE 2019/945
11. Ordine di servizio; dettagii missione e privacy
• Reg. UE 2019/947
OPERATIVA
12. Registrazione nel log operativo
• Art. UAS.SPEC.050 • Reg. UAS-IT (.9EC;. 050
POST-OPERATIVA
13. Riprese probatorie integrità file, catena custodia
• Art. 234-c.p.p. • Reg. UE 71 mss
VERIFICATO SU FONTI PRIMARIE: GDPR • D.Lgs. 51/2018 • Reg. UAS-IT • Cass. pen. 21557/2024

6. Le categorie operative ENAC/EASA: guida pratica

6.1 Categoria Aperta (Open)

È il regime ordinario per droni di peso inferiore a 25 kg. Non richiede autorizzazione ENAC per il singolo volo, ma impone requisiti minimi. La pianificazione parte sempre dalla verifica su D-Flight (ATM-09A) e dalla verifica delle restrizioni (ATM-03C).

Sottocategoria	UAS ammessi	Requisiti pilota	Limiti operativi
A1	< 250 g (C0) o < 900 g (C1)	Attestato A1/A3 (esame online ENAC)	Può sorvolare persone isolate (non assembramenti). No zone vietate. VLOS. Max 120 m.
A2	< 4 kg (C2)	Attestato A2 (esame in presenza)	Minima 30 m dalle persone (o 5 m in modalità bassa velocità). VLOS. Max 120 m.
A3	< 25 kg (C3-C4)	Attestato A1/A3 (esame online ENAC)	Min 150 m da zone abitate. No sorvolo persone. VLOS. Max 120 m.

DEFINIZIONE TECNICA: "ASSEMBRAMENTO" (art. 2 Reg. 2019/947): il Regolamento definisce "assembramenti di persone" come "raduni di persone in cui è impossibile disperdersi a causa dell'elevata densità dei presenti". NON è una definizione numerica: non esiste una soglia di persone. Il criterio è la POSSIBILITÀ DI DISPERSIONE. Esempi operativi: (a) non assembramento: piazza con persone che si muovono liberamente, mercato all'aperto con percorsi liberi, folla disposta su prato aperto; (b) assembramento: stadio riempito con accessi chiusi, corteo compresso in strada stretta senza via di fuga laterale, concerto in area recintata. In caso di dubbio, la valutazione è rimessa al pilota che, se la ritiene rischiosamente ambigua, deve astenersi o passare a Categoria Specifica con autorizzazione ENAC. LIMITE 120 M: si misura dal punto più vicino della SUPERFICIE terrestre (non dal livello del mare): su un colle, il limite di 120 m si conta dalla cima del colle. In prossimità di ostacoli artificiali > 105 m di altezza, è consentito volare fino a 15 m sopra l'ostacolo su richiesta scritta del gestore (UAS.OPEN.010 par. 3 Reg. 2019/947).

6.2 Categoria Specifica

Obbligatoria quando l'operazione non rientra nei parametri della Categoria Aperta (volo BVLOS, oltre 120 m, droni > 25 kg, ecc.). Richiede il Manuale delle Operazioni e una valutazione del rischio (metodologia SORA o scenari standard EU STS-EASA). Dal 1° gennaio 2026 gli scenari standard nazionali italiani (IT-STS-01 e IT-STS-02) sono definitivamente scaduti per effetto del Reg. (UE) 2022/425, art. 23, par. 4: le dichiarazioni rese su IT-STS hanno cessato di essere valide. I Comandi che operavano su base IT-STS devono adeguarsi agli scenari standard europei (EU STS-01/02) o richiedere Autorizzazione Operativa ENAC.

⚠ AGGIORNAMENTO– Transizione IT-STS → EU STS dal 1° gennaio 2026

Gli scenari standard nazionali IT-STS-01 e IT-STS-02 sono definitivamente cessati il 31 dicembre 2025. Base normativa: Reg. (UE) 2022/425, art. 23 par. 4 (testo verificato su EUR-Lex): "Tali dichiarazioni cessano di essere valide a decorrere dal 1° gennaio 2026". ENAC ha confermato il 31 dicembre 2025 come scadenza definitiva (Disposizione DG n. 73/2023 e pagina ENAC "Scenari standard nazionali", aggiornata luglio 2025). Non sono previste ulteriori proroghe.

Adempimenti richiesti ai Comandi di Polizia Locale dal 1° gennaio 2026: Verificare il proprio status sul portale D-Flight prima di qualsiasi operazione in Categoria Specifica. (a) I piloti devono possedere attestato teorico EU STS-01 e/o EU STS-02 + addestramento pratico + CRM + COM aeronautiche. (b) I droni utilizzati devono avere marcatura C5 (per EU STS-01) o C6 (per EU STS-02), oppure essere convertiti con terminatore di volo e paracadute certificati EASA. (c) Le dichiarazioni operative vanno aggiornate su D-Flight con riferimento agli EU STS anziché agli IT-STS. (d) In alternativa: richiedere Autorizzazione Operativa ENAC specifica, che non richiede droni C5/C6 ma impone un Risk Assessment SORA completo.

- Scenario Standard EU STS-01 EASA: volo VLOS in area urbana/suburbana, drone C5 obbligatorio (o C2/C3 convertito con terminatore di volo + paracadute EASA). In vigore dal 1° gennaio 2026 in sostituzione dell'IT-STS-01.
- Scenario Standard EU STS-02 EASA: volo BVLOS limitato con osservatore, aree non abitate, drone C6 obbligatorio. In vigore dal 1° gennaio 2026 in sostituzione dell'IT-STS-02.
- Autorizzazione Operativa ENAC: per operazioni al di fuori degli STS (BVLOS, notturno, aree non standard); richiede Risk Assessment SORA, Manuale delle Operazioni, documentazione tecnica. Non richiede marcatura C5/C6 ma procedura più complessa.
- LUC (Light UAS Operator Certificate): per enti che fanno uso frequente e sistematico di droni; richiede un Safety Management System

6.3 Volo di Stato (esenzione dalla normativa civile)

L'art. 2, par. 3, lett. a) del Reg. UE 2018/1139 esclude dall'ambito di applicazione della normativa civile EASA gli aeromobili usati per servizi di polizia, ricerca e soccorso, antincendio, controllo delle frontiere, sorveglianza costiera o servizi analoghi svolti nell'interesse pubblico da organismi abilitati da uno Stato membro. A livello di diritto interno, il percorso per la Polizia Locale è il seguente: i droni Polizia Locale sono per default aeromobili privati (art. 744 co. 2 CdN – verificato su fonte primaria), poiché la Polizia Locale non rientra nelle categorie ex art. 744 co. 1 (Forze di polizia dello Stato, Dogana, VVF, Dipartimento protezione civile). Per acquisire lo status di aeromobile di Stato occorre il Decreto MIT ex art. 746 co. 1 CdN, che equipara i droni adibiti a "servizio di Stato di carattere non commerciale". Con l'equiparazione: si ottiene l'esenzione dalle norme del Codice della Navigazione (art. 748 co. 1) e da tasse e tariffe aeroportuali (art. 748 co. 2); si opera con le regolamentazioni delle competenti Amministrazioni d'intesa con ENAC (art. 748 co. 3). Per ottenere il riconoscimento occorre presentare domanda formale al Ministero delle Infrastrutture e dei Trasporti (MIT). La qualificazione va trattata con cautela per la Polizia Locale comunale: non coincide automaticamente con "pubblica sicurezza" in senso statale. In ogni caso, gli obblighi GDPR e D.Lgs. 51/2018 restano integralmente applicabili.

La procedura di equiparazione ex art. 746 CdN ha registrato una significativa accelerazione nel biennio 2025-2026: il Ministero delle Infrastrutture e dei Trasporti (MIT) ha emesso decreti direttoriali in favore, tra gli altri, del Corpo di Polizia Locale dell'Unione Valdera (PI) con decreto n. 1 del 7 gennaio 2025, del Corpo di Polizia Locale del Comune di Bari con decreto n. 28 del 5 giugno 2025, e del Comune di Magenta (MI) con decreto del 19 gennaio 2026 (DJI Mini 4 Pro, per finalità di polizia giudiziaria, sicurezza urbana e controllo del territorio). Il fenomeno evidenzia che, mentre la via del Patto Prefetto-Sindaco resta necessaria per le finalità di sicurezza urbana ex D.L. 14/2017, la via dell'equiparazione MIT è percorribile in parallelo e consente esenzioni operative rilevanti (artt. 748 co. 1-2 CdN). Le due strade non si escludono a vicenda: un Comune può richiedere l'equiparazione MIT e contestualmente stipulare il Patto, ottenendo una copertura giuridica duale.

7. Casi studio reali 2024-2026

La tabella seguente riepiloga i casi reali più significativi in materia di droni e tecnologie di videosorveglianza della Polizia Locale, verificati sulle fonti primarie (provvedimenti Garante, atti parlamentari). Costituisce la base empirica su cui si fondano le raccomandazioni del capitolo “Raccomandazioni operative conclusive”.

Caso	Fonte primaria	Esito	Principio ricavabile
Treviso – droni Polizia Locale per pubblica sicurezza	Garante, Provv. n. 405 del 4.7.2024 (docweb 10050298)	Procedimento archiviato con statuizione di principio: la Polizia Locale non può usare droni per finalità di PS senza base giuridica specifica	Conferma la posizione restrittiva sull'uso PS. Quanto alle termocamere: il Garante ha archiviato perché nel caso concreto le sagome erano indistinguibili; non ha tuttavia affermato che la termografia sia per definizione esclusa dal perimetro dei dati personali — la qualificazione dipende dalla funzione e dal contesto (cfr. FAQ 9).
Orte – videosorveglianza senza DPIA	Garante, Provv. n. 10198694 (Comune di Orte)	Sanzione per assenza di DPIA e di retention policy	La mancanza di retention policy è sanzionata anche in assenza di danni concreti. La DPIA non è un documento di facciata: deve essere operativa.
Pescara – body cam Polizia Locale (parere negativo)	Garante, Provv. n. 743 del 4.12.2025 (docweb 10221993)	PARERE NEGATIVO (quarta versione DPIA). Motivi: criticità non adeguatamente chiarite relative all'uso di un sistema riferibile a un'azienda statunitense (rischio trasferimento dati extra-UE e modalità di accesso del fornitore ai dati), insufficienza dei chiarimenti tecnici forniti	Valido anche per droni: il cloud provider deve essere UE e non avere accesso in chiaro ai dati. Conferma esclusione Polizia Locale da D.P.R. 15/2018.
Comuni virtuosi – droni solo per finalità amministrative	Prassi consolidata (nessun procedimento Garante): uso droni per abusi edilizi, rilievi ambientali, incidenti stradali	Nessuna sanzione. Uso regolare e consolidato senza contestazioni	Per le finalità puramente amministrative il rischio giuridico è minimo se la DPIA è adottata e i dati non sono trattati per finalità di PS.
ANVU – risposta alla Prefettura di Lecce (18 feb. 2026)	Documento ANVU del 18 febbraio 2026 (disponibile su anvu.it). Risposta alla nota prefettizia prot. 0024109 del 12.2.2026	Contestazione giuridica della nota prefettizia; sostiene la legittimità dell’uso droni Polizia Locale per finalità proprie	Esprime la posizione estensiva. Non costituisce fonte normativa ma documento di categoria rilevante per il dibattito interpretativo (cfr. cap. 2.2).

8. Raccomandazioni operative conclusive

In considerazione dello stato del diritto al febbraio 2026, si raccomanda alle Polizie Locali di adottare il seguente approccio graduato per livello di rischio.

8.1 Adempimenti preliminari indispensabili (validi per OGNI finalità)

- Delibera/atto amministrativo che individui le finalità e ne giustifichi la necessità (proporzionalità GDPR)
- Registrazione del Comune come Operatore UAS su D-Flight (portale ENAC)
- Verifica che i piloti siano registrati e certificati: i dati dei piloti certificati presso i Centri di Addestramento ENAC (Entità Riconosciute) sono resi accessibili alle Autorità di Pubblica Sicurezza ai sensi dell'art. 28 comma 3 Reg. ENAC UAS-IT Ed. 1/2021 — il Comune può verificare tramite ENAC la validità degli attestati del proprio personale operativo
- Acquisto di UAS conformi alla classe CE appropriata
- Formazione dei piloti: attestato ENAC + formazione su scenari sensibili (spazi privati, assembramenti, contesti lavorativi)
- Polizza assicurativa RC con massimale minimo 750.000 DSP (~EUR 913.000)
- Nomina o designazione del DPO e suo coinvolgimento nella DPIA
- Redazione della DPIA (DPIA obbligatoria nella maggior parte degli impieghi operativi con telecamera, in particolare quando vi è monitoraggio sistematico di aree accessibili al pubblico; per finalità penali/PS: invio preventivo al Garante solo in presenza di rischio residuo elevato non mitigabile); consultare Garante Delibera 467/2018 (docweb 9058979) per l'elenco delle tipologie soggette a DPIA
- Adozione di un regolamento interno sull'uso dei droni: finalità ammesse, divieto controllo lavoratori, retention policy, accessi, sicurezza, catena di custodia, gestione incidenti e data breach
- Verifica prevolo su D-Flight delle zone geografiche (ATM-09A) e delle restrizioni (ATM-03C); per zone vietate ex art. 793 Cod. Nav.: autorizzazione ENAC + nulla osta del gestore/proprietario

8.2 Adempimenti aggiuntivi per finalità di sicurezza urbana (D.L. 14/2017)

Questo canale si applica esclusivamente alle finalità di sicurezza urbana ex D.L. 14/2017 (prevenzione criminalità diffusa su pubblica via). Non è utilizzabile come alternativa al canale L. 65/1986 per le funzioni ausiliarie di pubblica sicurezza in senso stretto, che richiedono il diverso procedimento descritto al cap. 8.3.

- Stipula del Patto per la sicurezza urbana tra Prefetto e Sindaco ex art. 5 D.L. 14/2017, con incluso il progetto droni come strumento di videosorveglianza su pubblica via
- Governance privacy documentata e allegata al patto (DPIA, informativa, retention policy, misure di sicurezza)
- Consultare la Circolare Ministero dell'Interno, Gabinetto del Ministro, Ufficio II – Ordine e Sicurezza Pubblica, circolare prot. 11001/123/111 (3), prot. uscita n. 0031004 del 7 aprile 2025, recante indicazioni applicative sui Patti per l'attuazione della sicurezza urbana e l'installazione di sistemi di videosorveglianza.

8.3 Adempimenti aggiuntivi per finalità ausiliarie di pubblica sicurezza (L. 65/1986)

Questo canale si applica esclusivamente alle funzioni ausiliarie di pubblica sicurezza ex L. 65/1986, attivabili solo su richiesta motivata del Questore o del Prefetto per specifiche operazioni. Non è sovrapponibile né fungibile con il Patto per la sicurezza urbana ex D.L. 14/2017, che persegue finalità diverse e produce una diversa catena di comando.

- Richiesta motivata scritta del Questore o del Prefetto per le specifiche operazioni (art. 3 L. 65/1986) -- NON è una "delega" in senso tecnico, ma una richiesta formale per specifiche operazioni che attiva il meccanismo ausiliario
- Disposizione del Sindaco che mette a disposizione il personale (art. 3 L. 65/1986)
- Atto formale di "messa a disposizione" scritto e protocollato: entrambi i passaggi (richiesta dell'autorità + disposizione del Sindaco) devono essere documentati prima dell'operazione
- Comunicazione al Prefetto e al Questore dell'identificazione del personale coinvolto e del tipo di drone utilizzato
- CATENA DI COMANDO (art. 5, co. 4 L. 65/1986): durante l'operazione il Comandante/personale Polizia Locale dipende operativamente dall'autorità di PS o dall'AG, non dal Sindaco; i log di volo e le immagini sono gestiti nell'ambito diretto di questa catena di comando e il Comandante non è autonomo nelle decisioni operative
- Ruoli privacy e governance del trattamento: definire per iscritto, prima dell'operazione, i ruoli e le responsabilità tra autorità richiedente e Comune/Comando, includendo almeno: finalità e perimetro; istruzioni operative; categorie di dati; modalità di raccolta e accesso; conservazione e cancellazione; misure di sicurezza; tracciabilità dei log; eventuali comunicazioni/trasferimenti a terzi. Evitare di qualificare automaticamente la relazione come "contitolarità" in assenza di una base normativa e di un assetto sostanziale coerente
- Applicazione del D.Lgs. 51/2018 per il trattamento dei dati a fini di law enforcement; DPIA preventiva (da inviare al Garante solo in presenza di rischio residuo elevato non mitigabile)
- Adozione di un protocollo tecnico-operativo condiviso con ENAC per le operazioni in contesto di pubblica sicurezza, definendo modalità di volo, aree operative e procedure di coordinamento con il controllo del traffico aereo.

8.4 Adempimenti per l'uso probatorio delle immagini

- Delimitare le riprese a luoghi pubblici o aperti al pubblico; tassativamente vietare la captazione di spazi di vita privata (art. 615-bis c.p.)
- Calcolare l'hash del file al momento dello scarico; conservare il file originale in formato non modificabile
- Redigere un verbale di acquisizione (missione,

data/ora, pilota, drone, hash, log di volo)
- Log tracciato di tutti gli accessi al file
- Verbale di consegna in caso di trasferimento all'AG o alle Forze di polizia

8.5 Adempimenti per ogni singola missione

- Emissione ordine di servizio/autorizzazione interna alla missione (vedi step 16 della tabella operativa)
- Verifica prevolo: meteo, D-Flight, NOTAM, presenza persone nell'area, restrizioni ATM-03C
- Registrazione della missione nel log operativo
- Se operazione in Categoria Specifica: è fortemente raccomandato compilare un Logbook del pilota (data, durata, tipo operazione) e predisporre un Drone Operation Plan (DOP) da conservare agli atti della missione, in coerenza con le prassi operative consolidate e con gli orientamenti in corso di formalizzazione da parte di ENAC. Monitorare gli aggiornamenti del Reg. ENAC UAS-IT per la formalizzazione di questi obblighi nel testo vigente
- In caso di incidente/inconveniente grave: notifica ANSV entro 60 minuti; valutare data breach GDPR (notifica al Garante entro 72 ore)

SUGGERIMENTO: è fortemente raccomandabile che ogni Comando di Polizia Locale adotti un “Regolamento per l'uso degli aeromobili a pilotaggio remoto” che includa: finalità ammesse per livello (amministrativa / sicurezza urbana / PS), titolo istituzionale richiesto per ciascuna, divieto uso per controllo lavoratori, divieto captazione spazi privati, procedure operative (ordine di servizio, log, catena di custodia), DPIA allegata, retention policy, procedura incidenti (ANSV + Garante). Tale regolamento, redatto con il DPO, costituisce la principale prova di accountability (art. 5, par. 2 GDPR) e riduce in modo significativo il rischio di responsabilità personale dei funzionari.

9. Indice delle fonti primarie consultate

Normativa europea

- Reg. (UE) 2018/1139 del Parlamento europeo e del Consiglio del 4 luglio 2018 (GUUE L 212/1 del 22.8.2018), come mod. da Reg. delegato (UE) 2021/1087 (GU L 236 del 5.7.2021) e Reg. (UE) 2024/2803 (GU L, 11.11.2024) -- versione consolidata 25.5.2025 -- artt. 2 par. 3 lett. a) (esclusione voli statali/polizia), 56 par. 8 (facoltà degli Stati di regolare uso UAS per ragioni di pubblica sicurezza), Allegato IX punti 1.1 e 1.3 (requisiti essenziali: conoscenza norme privacy e privacy by design obbligatorio)
- Reg. delegato (UE) 2019/945 della Commissione del 12 marzo 2019 (GUCE L 152 dell'11.6.2019), come mod. da Reg. (UE) 2020/1058 e (UE) 2022/1035
- Reg. di esecuzione (UE) 2019/947 della Commissione del 24 maggio 2019 (GUUE L 152 del 11.6.2019), come mod. da: Reg. 2020/639 (scenari standard STS-01/STS-02), Reg. 2020/746, Reg. 2021/1166 (proroga scenari nazionali), Reg. 2022/425 (proroga al 1.1.2026) -- versione consolidata 4.4.2022 -- artt. 2 (def. “assembramenti”: raduni impossibili da disperdere), 4 (requisiti Categoria Aperta), 14 (obbligo immatricolazione per UAS con sensori raccolta dati personali), 15 (zone geografiche), UAS.OPEN.010 (limite 120 m dalla superficie, eccezione ostacoli), UAS.OPEN.020 (esame A1/A3: privacy e protezione dati materia obbligatoria), Considerando 11 (conferma art. 56 par. 8 Reg. 2018/1139 nel regolamento attuativo)
- Reg. (UE) 2016/679 (GDPR) del 27 aprile 2016 (GUCE L 119 del 4.5.2016)
- Direttiva (UE) 2016/680 del 27 aprile 2016 (GUCE L 119 del 4.5.2016)

Normativa nazionale

- R.D. 30 marzo 1942, n. 327 (Codice della Navigazione), artt. 743-748, 793, 1174
- Legge 1° aprile 1981, n. 121 (Ordinamento Amministrazione PS), art. 16
- Legge 7 marzo 1986, n. 65 (Legge quadro Polizia Municipale), artt. 3, 5
- D.L. 18 febbraio 2015, n. 7, conv. L. 17 aprile 2015, n. 43, art. 5, co. 3-sexies
- D.L. 4 ottobre 2018, n. 113, conv. L. 1° dicembre 2018, n. 132, art. 35-sexies
- D.L. 20 febbraio 2017, n. 14, conv. L. 18 aprile 2017, n. 48 (c.d. Decreto Minniti), art. 5
- D.P.R. 15 gennaio 2018, n. 15 (G.U. n. 61 del 14 marzo 2018), artt. 1 c. 3, 6 cc. 1-2, 22, 23 cc. 3-4 e 24 cc. 4-5 -- la Polizia Locale è esclusa dall'ambito applicativo diretto ex art. 1 c. 3
- D.Lgs. 18 maggio 2018, n. 51
- D.Lgs. 10 agosto 2018, n. 101
- D.Lgs. 9 maggio 2005, n. 96 (modifica art. 793 Cod. Nav.)
- Legge 20 maggio 1970, n. 300 (Statuto dei Lavoratori), art. 4
- Codice di procedura penale, artt. 189, 234, 347
- Codice penale, art. 615-bis
- D.M. Interno 13 giugno 2022 (G.U. n. 192 del 18 agosto 2022)
- Regolamento ENAC UAS-IT, Edizione 1 del 4 gennaio 2021 e successive modifiche

Circolari e documenti tecnici ENAC

- ENAC, Circolare ATM-09A (Utilizzo dello spazio aereo per operazioni UAS e zone geografiche)
- ENAC, Circolare ATM-03C (Zone soggette a restrizioni delle attività di volo)
- ENAC, Nota prot. 31/07/2024-0113702 e -0113713 (Chiarimenti MTOM)
- ENAC, Nota sull'esenzione ex art. 71, par. 1 Reg. (UE) 2018/1139
- ENAC, Linee Guida LG-2023/005-UAS e LG-2023-006/UAS

Provvedimenti del Garante Privacy e linee guida

- Garante Privacy, Provvedimento n. 405 del 4 luglio 2024 (Comune di Treviso), docweb 10050298 -- DRONI: archiviazione con statuizione di principio sul divieto implicito alla Polizia Locale per uso PS; APP TrevisoSicura: sanzione EUR 7.000 per violazioni GDPR (le due vicende non vanno confuse)

- Garante Privacy, Provvedimento n. 234 dell'11 aprile 2024 (Comune di Madignano — videosorveglianza e informativa, docweb 10013356)
- Garante Privacy, Provvedimento n. 669 del 13 novembre 2025 (Comune di Orte — videosorveglianza, DPIA e conservazione, docweb 10198694)
- Garante Privacy, Comunicato stampa 3 settembre 2021 su istruttorie droni (docweb 9696781)
- Garante Privacy, Delibera n. 467 dell'11 ottobre 2018 (G.U. n. 269 del 19 novembre 2018, docweb 9058979) -- Elenco delle tipologie di trattamenti soggetti a DPIA obbligatoria ex art. 35, par. 4, GDPR; categorie rilevanti per i droni: monitoraggio sistematico di aree pubbliche, trattamento dati su reati, sistemi di controllo a distanza lavoratori, soggetti vulnerabili, raccolta dati tramite reti
- EDPB (European Data Protection Board), Linee Guida 3/2019 sulla videosorveglianza
- WP29 (Gruppo di Lavoro art. 29 -- ora sostituito dall'EDPB), Parere 01/2015 "privacy e utilizzo di droni" (01673/15/IT WP231), adottato il 16 giugno 2015 -- unico documento istituzionale europeo specifico per droni e contrasto penale; i paragrafi §3.2 (contrasto penale) e §5.4 (10 condizioni operative) sono stati verificati; inquadramento: fonte interpretativa pre-GDPR, parzialmente aggiornata da EDPB 3/2019 per profili generali
- Garante Privacy, Provvedimento n. 743 del 4 dicembre 2025 (Comune di Pescara – body cam Polizia Locale), docweb 10221993 – PARERE NEGATIVO sulla DPIA body cam Polizia Locale per finalità ausiliarie di PS; conferma esclusione Polizia Locale da D.P.R. 15/2018; richiede archiviazione cloud in UE e cifratura end-to-end
- Garante Privacy, FAQ Videosorveglianza – Il Vademecum

Iter legislativo riforma L. 65/1986 – atti parlamentari verificati

Camera dei deputati, C. 1716 (Governo Piantedosi, 16 feb. 2024) e abb. C. 125, 600, 875, 1727, 1862 – Comm. I Affari Costituzionali, in sede referente; testo base adottato il 3 dicembre 2025 [verificato su camera.it, aggiornato al 28.2.2026]. Senato della Repubblica, S. 883 (Gasparri, FI, 20 sett. 2023) – assegnato, esame non ancora iniziato [verificato su senato.it]. Senato della Repubblica, S. 704 (Romeo, Lega, 16 maggio 2023) – assegnato, esame non ancora iniziato [verificato su senato.it].

Giurisprudenza

- Cass. pen., Sez. IV, sent. n. 21557/2024 (videoriprese in luoghi pubblici, utilizzabilità come prova)
- Cass. pen., Sez. III, sent. n. 50919/2019 (videosorveglianza lavorativa e responsabilità penale)

Legislazione sicurezza del lavoro

- D.Lgs. 9 aprile 2008, n. 81 (Testo Unico in materia di salute e sicurezza nei luoghi di lavoro -- TUSL), artt. 17 co. 1 lett. a) (DVR non delegabile), 28 (contenuto DVR), 36-37 (informazione e formazione dei lavoratori); come modificato da D.Lgs. 106/2009 e successive integrazioni -- applicabile a tutti i settori pubblici e privati senza eccezioni; il Comune che impiega piloti UAS è datore di lavoro obbligato a includere l'attività nel DVR e a garantire la formazione specifica

Documenti istituzionali e di categoria

- Ministero dell'Interno - Protocollo Viminale-ENAC su droni alle Forze di polizia
- Ministero dell'Interno, Gabinetto del Ministro, Ufficio II – Ordine e Sicurezza Pubblica, circolare prot. 11001/123/111 (3), prot. uscita n. 0031004 del 7 aprile 2025, recante indicazioni applicative sui Patti per l'attuazione della sicurezza urbana ex art. 5 D.L. 14/2017 e l'installazione di sistemi di videosorveglianza
- Prefettura di Lecce, nota prot. 0024109 del 12 febbraio 2026
- Ministero dell'Interno, Nota prot. 555/O./0001054/2020/2 del 30 marzo 2020 (uso droni COVID-19)
- ANVU (Associazione Professionale Polizia Locale d'Italia), Documento 18 febbraio 2026
- M. Lamon - M. Bonazzi, "I droni a supporto della pubblica sicurezza", in GIURETA - Rivista di Diritto dell'Economia, dei Trasporti e dell'Ambiente, Vol. XIX, 2021 (ISSN 1724-7322) -- fonte dottrinale verificata per la ricostruzione del D.P.R. 15/2018

Portali online verificati: ENAC (www.enac.gov.it), D-Flight (www.d-flight.it), Garante Privacy (www.garanteprivacy.it), EUR-Lex (eur-lex.europa.eu), Normattiva (www.normattiva.it), Gazzetta Ufficiale (www.gazzettaufficiale.it).

Documento aggiornato al 1° marzo 2026.

Per aggiornamenti normativi consultare: www.enac.gov.it | www.garanteprivacy.it | www.normattiva.it

Appendice — Domande Frequenti (FAQ)

Le seguenti FAQ raccolgono le domande più ricorrenti che pervengono ai Comandi di Polizia Locale in merito all'utilizzo operativo dei droni. Le risposte sono basate sul quadro normativo vigente al 1° marzo 2026 e sui provvedimenti delle autorità competenti illustrati nelle sezioni precedenti. Per i riferimenti normativi puntuali si rinvia alle sezioni corrispondenti del presente documento.

A. Normativa ENAC e obblighi operativi (Remote ID, D-Flight, scenari STS)

FAQ 1 — Il Comune deve registrarsi su D-Flight anche per droni sotto i 250 g?

Sì, se il drone è dotato di telecamera, microfono o qualsiasi altro dispositivo in grado di captare dati personali. In tal caso la registrazione come Operatore UAS su D-Flight è obbligatoria indipendentemente dal peso, ai sensi del Reg. UAS-IT ENAC, artt. 6 e 9, e delle FAQ ENAC (punto 8). All'esito della registrazione il Comune riceve un Operator Registration ID (QR code) da apporre su ciascun drone. I droni sotto 250 g privi di tali dispositivi sono invece esenti dall'obbligo di registrazione.

FAQ 2 — Cos'è il Remote ID e chi è obbligato ad averlo?

Il Remote ID è un sistema elettronico che trasmette in tempo reale, via Bluetooth o Wi-Fi, i dati identificativi del drone e dell'operatore durante il volo. È obbligatorio dal 1° gennaio 2024 per tutti i droni di Classe C1 e superiori, nonché per quelli operanti in Categoria Specifica (inclusi i legacy privi di marcatura di classe), ai sensi del Reg. delegato (UE) 2019/945, artt. 11 ss. Solo le forze dell'ordine possono decodificare l'identità dell'operatore a partire dal codice trasmesso; i comuni cittadini ricevono esclusivamente dati anonimi.

FAQ 3 — Gli scenari IT-STS-01 e IT-STS-02 sono ancora validi nel 2026?

No. Gli scenari standard nazionali IT-STS-01 e IT-STS-02 sono definitivamente cessati il 31 dicembre 2025, in applicazione del Reg. (UE) 2022/425, art. 23, par. 4. Dal 1° gennaio 2026 le operazioni già dichiarate in base a IT-STS devono essere riadeguate agli scenari EASA (STS-01 e STS-02) oppure devono ottenere un'autorizzazione operativa ENAC. I Comuni che non abbiano aggiornato le proprie dichiarazioni operano attualmente in assenza di copertura normativa: è necessario verificare il proprio status sul portale D-Flight e, ove necessario, presentare nuova dichiarazione STS-EASA.

B. Competenze della Polizia Locale: cosa può e cosa non può fare

FAQ 4 — La Polizia Locale può usare il drone per finalità di pubblica sicurezza (prevenzione reati)?

È il punto più controverso del quadro normativo vigente. La posizione del Ministero dell'Interno (circ. n. 557/PAS/U/013395/15900.D.2 del 3 agosto 2021) è restrittiva: le funzioni di pubblica sicurezza spettano in via esclusiva alle Forze di polizia dello Stato ex art. 1 L. 121/1981, e la Polizia Locale non è inclusa nell'elenco di cui all'art. 16 L. 121/1981. Il Garante Privacy ha avvalorato questa tesi con il Provv. n. 405/2024 (Comune di Treviso). La posizione estensiva dell'ANVU ammette invece un uso della Polizia Locale per finalità ausiliarie, purché vi sia una formale delega del Questore o del Prefetto ai sensi dell'art. 3 L. 65/1986. In assenza di tale delega, il rischio di illegittimità è elevato.

FAQ 5 — Il drone può essere usato per la "sicurezza urbana integrata" ex D.L. 14/2017?

Sì, ma solo previo Patto per la Sicurezza Urbana stipulato tra il Sindaco e il Prefetto ai sensi degli artt. 5-7 del D.L. 14/2017 (conv. L. 48/2017), che attribuisca espressamente alla Polizia Locale il compito di monitoraggio del territorio con sistemi aerei. Il Patto deve identificare le aree geografiche, le finalità e le modalità operative. In assenza del Patto, l'uso del drone per finalità di sicurezza urbana ex D.L. 14/2017 non è coperto da base giuridica adeguata. Questo vale specificamente per la sicurezza urbana: per le funzioni ausiliarie di pubblica sicurezza in senso stretto, il titolo giuridico è invece la richiesta motivata ex L. 65/1986, che segue un procedimento distinto descritto al cap. 8.3.

FAQ 6 — Per quale tipo di attività la Polizia Locale può sicuramente usare il drone senza autorizzazioni particolari?

Per le finalità prettamente amministrative: rilievi edilizi, sopralluoghi ambientali, rilievi di incidenti stradali, abusi edilizi, mappatura catastale, monitoraggio eventi pubblici a fini organizzativi, ispezioni di infrastrutture. In questi casi la base giuridica è l'art. 6, par. 1, lett. e) GDPR (compito di interesse pubblico), non è richiesta la qualifica di Forza di polizia ai sensi della L. 121/1981, ma restano obbligatori: DPIA (per il monitoraggio sistematico di aree pubbliche ex Delibera Garante 467/2018), informativa ex artt. 13-14 GDPR e registrazione su D-Flight.

C. Privacy, GDPR e adempimenti del Garante

FAQ 7 — La DPIA è sempre obbligatoria prima di usare il drone?

Sì, per la quasi totalità degli impieghi operativi della Polizia Locale. La Delibera del Garante n. 467 del 2018 include tra i trattamenti soggetti obbligatoriamente a DPIA: (a) il monitoraggio sistematico di aree pubbliche, (b) il trattamento di dati su reati e misure di sicurezza, (c) i sistemi di sorveglianza con tecnologie innovative. Tutti e tre i criteri ricorrono tipicamente nell'uso del drone da parte della Polizia Locale. L'unica eccezione sono i voli sporadici per rilievi tecnici puntuali (es. un singolo sopralluogo edilizio) che non configurano "monitoraggio sistematico": in tal caso la DPIA è raccomandata ma non strettamente obbligatoria.

FAQ 8 — Cosa ha stabilito il Garante nel caso del

Comune di Treviso?

Con il Provvedimento n. 405 del 4 luglio 2024 (docweb 10050298), il Garante ha archiviato il procedimento sul drone termico della Polizia Locale di Treviso, ma solo perché il sistema produceva "sagome indistinguibili" non idonee all'identificazione dei soggetti. Nel medesimo provvedimento il Garante ha affermato il principio che la Polizia Locale non ha titolo a svolgere attività di pubblica sicurezza con droni in assenza di delega formale delle Forze di polizia statali, costituendo questo un limite assoluto di competenza, non solo di proporzionalità del trattamento dati. Le sanzioni per l'app TrevisoSicura (EUR 7.000 per violazioni GDPR) sono un procedimento distinto.

FAQ 9 — Il drone termico è soggetto al GDPR?

Dipende dalla funzione concreta e dal contesto operativo, non solo dalle caratteristiche tecniche del sensore. Nel caso Treviso (Provv. n. 405/2024), il Garante ha archiviato il procedimento tenendo conto delle circostanze dichiarate dal Comune — in particolare che le sagome erano indistinguibili e che il sistema non era idoneo all'identificazione in quel contesto specifico. Il Garante non ha tuttavia affermato che la termografia sia per definizione esclusa dal perimetro dei dati personali: ha anzi ribadito nel medesimo provvedimento che l'impiego di droni con termocamere *può comportare* trattamento di dati personali, anche relativi a reati, e che la Polizia Locale non aveva titolo per quell'uso in assenza di base giuridica adeguata. La valutazione va quindi condotta caso per caso: rileva non solo la risoluzione del sensore, ma anche se le immagini siano utilizzate per selezionare soggetti da sottoporre a controllo, se siano incrociate con altre banche dati, se consentano identificazione indiretta nel contesto specifico. In caso di dubbio, è obbligatorio procedere come se il GDPR si applicasse e condurre la DPIA.

D. Volo di Stato e procedura di equiparazione ex art. 746 Cod. Nav.

FAQ 10 — Cos'è il "Volo di Stato" e la Polizia Locale può ottenerlo?

Il Volo di Stato è la qualifica che sottrae l'aeromobile alla normativa civile EASA/ENAC, ai sensi dell'art. 2, par. 3, lett. a) del Reg. (UE) 2018/1139 e dell'art. 744 del Codice della Navigazione. Si applica agli aeromobili "impegnati in operazioni militari, doganali, di polizia, antincendio, ricerca e soccorso o servizi analoghi svolti nell'interesse pubblicò". La Polizia Locale può ottenerlo tramite la procedura di equiparazione disciplinata dall'art. 746 CdN, che richiede un decreto direttoriale del Ministero delle Infrastrutture e dei Trasporti (MIT), previa verifica dei requisiti tecnici e operativi. I Comuni non possono rivendicare la qualifica di Volo di Stato in via autonoma, senza il decreto MIT.

FAQ 11 — Come si avvia la procedura di equiparazione ex art. 746 CdN?

Il Comune presenta istanza al Ministero delle Infrastrutture e dei Trasporti (MIT), Direzione Generale per gli Aeroporti e la Sicurezza del Volo, allegando: (a) descrizione del drone e dei sistemi di bordo, (b) finalità operative per cui si chiede l'esenzione, (c) documentazione tecnica del costruttore, (d) evidenza delle qualifiche del personale. Il Ministero delle Infrastrutture e dei Trasporti (MIT) esamina l'istanza e, se sussistono i requisiti, emette un decreto direttoriale nominativo. Esempi recenti: Unione Valdera (PI), decreto MIT n. 1 del 7 gennaio 2025; Comune di Bari, decreto n. 28 del 5 giugno 2025; Comune di Magenta (MI), decreto del 19 gennaio 2026. La procedura è compatibile con il Patto per la Sicurezza Urbana e le due strade possono essere percorse in parallelo.

E. Uso probatorio delle riprese

FAQ 12 — Le riprese del drone sono utilizzabili come prova in un procedimento penale?

Sì, se acquisite su luoghi pubblici o aperti al pubblico e nel rispetto della normativa vigente. La giurisprudenza consolidata (Cass. pen., Sez. IV, n. 21557/2024) qualifica le riprese su luoghi pubblici come "prova documentale" ex art. 234 c.p.p., non come intercettazione, e le ritiene pienamente utilizzabili. Sono invece inutilizzabili — e costituiscono il reato di cui all'art. 615-bis c.p. — le riprese che captino l'interno di abitazioni private o luoghi di privata dimora, anche se effettuate dall'esterno con ottiche potenti o in visione termica.

FAQ 13 — Quali sono i requisiti minimi per la catena di custodia dei file video?

Affinché le riprese siano ammissibili e resistano a eventuali eccezioni difensive, è necessario: (a) conservare i file in formato originale senza alterazioni (hash MD5/SHA-256 da calcolare subito dopo l'atterraggio); (b) compilare un verbale di volo che documenti data, ora, coordinate GPS, quota, operatore, finalità, durata e area di ripresa; (c) conservare i metadati EXIF/telemetria del drone; (d) trasferire i file su supporto sicuro con accesso controllato (log degli accessi); (e) rispettare i termini di conservazione previsti nella DPIA, con cancellazione automatica allo scadere. La mancanza di uno di questi elementi non determina automaticamente l'inutilizzabilità, ma espone a eccezioni difensive sulla genuinità della prova.

F. Responsabilità e sanzioni

FAQ 14 — Quali sanzioni rischiano i responsabili in caso di uso illegittimo del drone?

Il quadro sanzionatorio è articolato su tre livelli. Sul piano penale: chi usa il drone per captare immagini all'interno di luoghi di privata dimora commette il reato di interferenze illecite nella vita privata (art. 615-bis c.p.), punito con la reclusione da 6 mesi a 4 anni, aggravata per il pubblico ufficiale che agisce con abuso dei poteri. Sul piano amministrativo-GDPR: il Garante può irrogare sanzioni pecuniarie fino a EUR 20.000.000 o al 4% del fatturato annuo mondiale (art. 83 GDPR) agli enti, e richiedere la cancellazione dei dati. Sul piano

della responsabilità civile-erariale: il responsabile del procedimento e il Comandante del Corpo possono essere chiamati a rispondere del danno erariale derivante da eventuali risarcimenti a terzi.

FAQ 15 — L'ente è responsabile anche se l'operatore ha agito di propria iniziativa?

In linea di principio sì, salvo che l'ente dimostri di aver adottato tutte le misure organizzative idonee a prevenire la condotta illecita (art. 5 GDPR; principio di accountability). Questo significa che la responsabilità dell'ente si riduce — ma non si esclude automaticamente — se sono stati predisposti: regolamento interno per l'uso dei droni, formazione specifica degli operatori, DPIA aggiornata, designazione del DPO (ove obbligatoria), sistema di log e audit delle missioni. In assenza di tali misure, il Comune risponde a titolo di culpa in organizzando e l'operatore a titolo personale. Si raccomanda quindi di formalizzare le procedure interne prima di qualsiasi impiego operativo del drone.