FRIA

Fundamental Rights Impact Assessment
Sistema di Video Analisi
Comune di Mirandola

Data di approvazione:

Sommario

Definizioni

AI Act (Regolamento UE 2024/168G)
Normativa europea che stabilisce regole armonizzate sull'intelligenza artificiale, con l'obiettivo di garantire sicurezza, trasparenza, qualità dei dati, supervisione umana e gestione dei rischi, soprattutto per i sistemi ad alto rischio.

Alto rischio (High-Risk AI System)
Categoria di sistemi IA individuata dall'AI Act, soggetti a requisiti più stringenti. La valutazione del rischio dipende dal settore di impiego, dalla finalità del sistema e dai possibili impatti su diritti fondamentali, salute, sicurezza o ordine pubblico.

DPIA (Data Protection Impact Assessment)
Valutazione d'impatto sulla protezione dei dati prevista dall'art. 35 GDPR. Ha come obiettivo l'analisi dei rischi per i dati personali e l'individuazione delle misure di mitigazione.

FRIA (Fundamental Rights Impact Assessment)
Valutazione d'impatto sui diritti fondamentali introdotta dall'AI Act. Complementare alla DPIA, serve a valutare gli effetti di un sistema IA sui diritti fondamentali delle persone (libertà, dignità, sicurezza, non discriminazione).

Fornitore (Provider)
Chi sviluppa, produce o commercializza un sistema di IA con il proprio nome o marchio. È responsabile della conformità tecnica del sistema ai requisiti del Regolamento.

Deployer (Utilizzatore)
Soggetto (es. Comune, ente pubblico o azienda) che utilizza il sistema di IA nel proprio contesto operativo. Ha responsabilità organizzative e di sorveglianza umana, nonché l'obbligo di svolgere la FRIA.

GDPR (Regolamento UE 2016/67G)
Regolamento generale sulla protezione dei dati personali. Garantisce i diritti e le libertà fondamentali delle persone connessi al trattamento dei dati.

IMT (Indice di Monitoraggio Territoriale)
Fattore di correzione che pesa variabili come area sorvegliata, numero di telecamere, densità di popolazione e frequenza di utilizzo, per calcolare l'intensità del monitoraggio su un territorio.

IR (Impatto Residuo)
Valore dell'impatto sui diritti fondamentali rimasto dopo l'applicazione delle misure di mitigazione.

Log
Registrazioni automatiche delle attività del sistema (accessi, attivazioni di alert, modifiche di configurazione). Servono per audit, accountability e tracciabilità.

Mitigazione (Misure di)
Azioni tecniche e organizzative volte a ridurre il rischio e l'impatto sui diritti fondamentali (es. trasparenza, supervisione umana, cifratura, minimizzazione dei dati).

PI Base (Potenziale Impatto di Base)
Indice iniziale che misura il potenziale impatto sui diritti e libertà fondamentali, prima dell'applicazione di misure di mitigazione.

PIT (Potenziale Impatto sul Territorio)
Valore ottenuto moltiplicando il PI Base per l'IMT. Indica l'impatto complessivo tenendo conto del contesto territoriale e della capacità di monitoraggio.

Profilazione
Qualsiasi trattamento automatizzato di dati personali che valuta aspetti personali di una persona fisica (comportamento, spostamenti, preferenze, affidabilità). È un'attività sensibile e può far ricadere un sistema tra quelli ad alto rischio.

Supervisione umana (Human-in-the-loop)
Principio secondo cui ogni decisione rilevante generata dall'IA deve essere validata da un operatore umano prima di produrre effetti concreti o giuridici.

1. SCOPO E CONTESTO DELLA FRIA

1.1 Premessa

La presente FRIA valuta l'impatto sui diritti e le libertà fondamentali delle persone derivante dall'uso, da parte del Comune, di un sistema di videosorveglianza con funzionalità di videoanalisi IA (VideoAnalisi LIVE basato su iSentry).
Il documento si basa sulle informazioni tecniche fornite nella FRIA del produttore che vengono adattate al contesto dell'Ente pubblico ed all'affettivo utilizzo dell'impianto di videosorveglianza da parte del Comune.
Un sistema di intelligenza artificiale è un software progettato per elaborare dati e generare output come previsioni, raccomandazioni o decisioni, influenzando ambienti o persone. Utilizza tecniche e modelli, compreso l'apprendimento automatico, per individuare schemi, interpretare informazioni e svolgere compiti complessi. Può operare in modo autonomo o assistito, con diversi livelli di intervento umano nel processo decisionale.
L'impiego di sistemi di intelligenza artificiale nella videosorveglianza per la sicurezza urbana può risultare utile per diversi motivi:

- Maggiore capacità di rilevamento: l'IA può analizzare in tempo reale grandi quantità di immagini e flussi video, individuando comportamenti anomali, oggetti sospetti o situazioni potenzialmente pericolose con rapidità superiore a quella umana.
- Prevenzione e intervento tempestivo: l'analisi automatica consente di generare allerte immediate, permettendo alle forze di polizia locale di intervenire prima che un evento degeneri.
- Supporto alle indagini: le funzioni di ricerca intelligente e tracciamento facilitano la ricostruzione degli eventi e l'individuazione di responsabili, migliorando l'efficacia investigativa.
- Copertura continua: i sistemi possono operare 24/7 senza cali di attenzione, garantendo un monitoraggio costante delle aree urbane.

Il Comune è Responsabile della gestione operativa del sistema, dell'informativa ai cittadini e della supervisione umana prima dell'adozione di decisioni che si basano sulla videoanalisi.

Tutela dei diritti fondamentali delle persone

Il bilanciamento tra sicurezza urbana e diritti fondamentali riconosciuti dalla Carta dell'UE richiede che le misure adottate siano utili allo scopo, limitate allo stretto necessario e il meno invasive possibile.
La videosorveglianza con sistemi di IA deve concentrarsi solo su situazioni di reale rischio, evitare controlli indiscriminati sulla popolazione e prevedere sempre un controllo umano prima di agire, così da proteggere libertà e dignità delle persone garantendo al tempo stesso la sicurezza.

Ambiti di applicazione di GDPR e AI ACT

IL GDPR tutela il diritto alla riservatezza delle persone fisiche, introducendo i seguenti principi:

Trasparenza: Ai sensi dell'Art. 13 e 14 del GDPR, le aziende devono informare gli interessati non solo dell'uso di sistemi di IA, ma anche della logica sottostante alle decisioni automatizzate e delle conseguenze che queste possono avere. In particolare, l'Art. 22 del GDPR vieta le decisioni basate unicamente sul trattamento automatizzato, inclusa la profilazione, che producano effetti giuridici o significativi per l'interessato.

Minimizzazione dei dati: Il principio di minimizzazione (Art. 5, par. 1, lett. c del GDPR) è cruciale. I sistemi di IA devono essere progettati per raccogliere e trattare solo i dati strettamente necessari per la specifica finalità, evitando la raccolta eccessiva e non pertinente.

Diritto di revisione umana: L'Art. 22 del GDPR stabilisce il diritto dell'interessato a non essere sottoposto a una decisione basata unicamente su un trattamento automatizzato. Questo garantisce il diritto a una revisione umana, a contestare la decisione e a ottenere l'intervento di un operatore.

Valutazione d'Impatto sulla Protezione dei Dati (DPIA): La DPIA è un requisito fondamentale (Art. 35 del GDPR) per i sistemi di IA che presentano rischi elevati per i diritti e le libertà delle persone.
Tale valutazione deve analizzare la natura, l'ambito, il contesto e le finalità del trattamento, identificando i rischi e le misure per mitigarli.

Base Giuridica: Ogni trattamento di dati personali da parte di un sistema di IA deve avere una valida base giuridica (Art. 6 del GDPR), come il consenso, l'esecuzione di un contratto o un legittimo interesse. Per le decisioni automatizzate, la base giuridica deve essere particolarmente solida.

L'AI Act: Un Nuovo Quadro di Responsabilità

A integrazione del GDPR, l'AI Act stabilisce un quadro normativo specifico per lo sviluppo, la commercializzazione e l'uso dell'intelligenza artificiale all'interno dell'Unione Europea. Il suo obiettivo primario è garantire che l'IA sia sicura, etica e rispettosa dei diritti fondamentali.

Classificazione dei sistemi IA: L'AI Act classifica i sistemi di IA in base al rischio che comportano, con categorie che vanno dal rischio inaccettabile (totalmente vietato, ad es. sistemi di sorveglianza sociale), al rischio elevato (soggetti a requisiti stringenti), fino al rischio minimo (con obblighi limitati). Le aziende che utilizzano sistemi ad alto rischio, come quelli in ambito medico, di selezione del personale o di gestione dei trasporti, sono soggette a rigide verifiche e obblighi.

Obblighi per i fornitori e gli utilizzatori: L'AI Act impone doveri specifici a chi sviluppa (fornitori) e a chi utilizza (utilizzatori) sistemi di IA. Questi obblighi includono la valutazione e mitigazione dei rischi, l'adozione di un sistema di gestione della qualità, la registrazione e la trasparenza algoritmica, e la sorveglianza post-commercializzazione per monitorare il comportamento del sistema dopo il suo lancio.

Sanzioni: L'AI Act prevede sanzioni severe per le violazioni, che possono arrivare fino a 35 milioni di euro o il 7% del fatturato globale (a seconda di quale sia maggiore), a testimonianza della serietà con cui l'UE affronta i rischi dell'IA

Il Regolamento Generale sulla Protezione dei Dati (GDPR) e l'AI Act operano in stretta connessione, affrontando due dimensioni complementari della stessa realtà. Il GDPR si concentra sulla protezione dei dati personali e sulla tutela dei diritti e delle libertà fondamentali delle persone rispetto al trattamento di tali dati, imponendo principi come liceità, correttezza, trasparenza, minimizzazione e limitazione della conservazione.

L'AI Act, quindi, introduce un quadro normativo specifico per i sistemi di intelligenza artificiale, con l'obiettivo di garantire sicurezza, trasparenza, qualità dei dati, supervisione umana e gestione dei rischi, soprattutto per i sistemi ad alto rischio.

Quando un sistema di IA elabora dati personali, entrambi i regolamenti si applicano in modo complementare: il GDPR stabilisce le basi giuridiche e le regole per il trattamento dei dati, mentre l'AI Act definisce gli standard tecnici e organizzativi per assicurare che lo sviluppo, la fornitura e l'uso dell'IA non compromettano diritti e libertà fondamentali. In pratica, la conformità al GDPR non è sufficiente per essere conformi all'AI Act, e viceversa: occorre predisporre, affiancare od eventualmente integrare le valutazioni d'impatto privacy (DPIA) con le valutazioni d'impatto sui diritti fondamentali (FRIA) previste dall'AI Act, assicurando un approccio coordinato che tenga conto sia della protezione dei dati sia della gestione complessiva dei rischi legati all'IA.

1.2 Oggetto della valutazione

La presente valutazione di impatto sui diritti fondamentali degli individui è inerente all'utilizzo di apparati dotati di tecnologie di Intelligenza Artificiale utilizzati dal Comune di Mirandola per la:

VideoAnalisi LIVE di un sistema di videosorveglianza per la sicurezza urbana

Finalità:

A) Videosorveglianza per la sicurezza urbana (telecamere fisse e mobili)

1. prevenire e reprimere atti delittuosi, attività illecite ed episodi di microcriminalità commessi sul territorio comunale, al fine di garantire maggiore sicurezza ai cittadini nell'ambito del più ampio concetto di "sicurezza urbana" di cui all'articolo 4 del decreto legge n. 14/2017 e delle attribuzioni del Sindaco in qualità di autorità locale di cui all'art. 50 e di ufficiale di governo di cui all'art. 54 comma 4 e 4-bis del d.lvo 267/2000;
2. prevenire e reprimere ogni tipo di illecito, di natura penale o amministrativa, in particolare legato a fenomeni di degrado e svolgere i controlli volti ad accertare e sanzionare le violazioni delle norme contenute nel regolamento di polizia urbana, nei regolamenti locali in genere e nelle ordinanze sindacali;
3. vigilare sull'integrità, sulla conservazione e sulla tutela del patrimonio pubblico e privato,
4. tutelare l'ordine, il decoro e la quiete pubblica;
5. controllare aree specifiche del territorio comunale;
6. monitorare i flussi di traffico;
7. verificare e calibrare il sistema di gestione centralizzata degli impianti semaforici

B) Telecamere lettura targhe:
   1. Verificare circolazione senza assicurazione, o con revisione scaduta; ricerca automezzi oggetto di indagine (su incarico dell'AG)

C) Fototrappole:
   1. Contrastare e sanzionale l'abbandono abusivo dei rifiuti

1.2 Normative e disposizioni di riferimento

a. Regolamento (UE) 2024/1689 (AI Act) e relative disposizioni sugli obblighi di trasparenza, supervisione umana e analisi dei rischi.
b. Regolamento (UE) 2016/679 (GDPR) e normative nazionali in materia di protezione dei dati personali e privacy.
c. Direttiva (UE) 2016/680 per la protezione delle persone fisiche riguardo al trattamento dei loro dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati e per l'esecuzione di sanzioni penali.
d. Linee guida WP 251 per la profilazione delle persone fisiche.
e. Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679 adottata dal 2 febbraio 2018 – Garante Privacy.
f. Provvedimento del Garante del 10 aprile 2025 in relazione all'utilizzo di sistemi AI (Artificial Intelligence) nella videosorveglianza.
g. Decreto-Legge 11 aprile 2025, n. 48 – "Disposizioni urgenti in materia di sicurezza pubblica, di tutela del personale in servizio, nonché di vittime dell'usura e di ordinamento penitenziario".
h. D.P.C.M. 12 gennaio 2024, recante "Piano triennale per l'informatica nella pubblica amministrazione 2024-2026" sulla base del quale è garantita l'adozione di Linee Guida sulla raccolta e il trattamento di dati finalizzati all'utilizzo in sistemi AI.
i. Linee guida della Commissione Europea del 18 luglio 2025 "Linee guida sulla portata degli obblighi per i modelli di intelligenza artificiale di uso generale stabiliti dalla legge sull'intelligenza artificiale".
j. Eventuali normative nazionali specifiche per i sistemi di videosorveglianza (decreti interni, provvedimenti del Garante Privacy).

1.3 I ruoli nella catena del valore dell'IA

La catena del valore dell'IA coinvolge diversi soggetti che ricoprono ruoli fondamentali nelle fasi di sviluppo, distribuzione e utilizzo delle tecnologie di IA. La presente FRIA adotta le definizioni di fornitore (provider) e deployer fornite dall'AI Act nel contesto generale dei sistemi di IA.

- Il fornitore è il soggetto che sviluppa un sistema di IA o un modello GPAI o che fa sviluppare un sistema di IA o un modello GPAI e immette tale sistema o modello sul

mercato o mette in servizio il sistema di IA con il proprio nome o marchio. Ha la responsabilità di garantire che il sistema di IA soddisfi i requisiti essenziali (sicurezza, robustezza, qualità dei dati, documentazione), esegua i test di conformità e rilasci la dichiarazione CE.

- Il deployer, che utilizza il sistema, anche integrandolo nei propri sistemi, senza modificarne in modo significativo il funzionamento. Non deve ripetere la certificazione di conformità, ma deve vigilare sul funzionamento quotidiano dell'IA e valutare gli impatti specifici sul proprio contesto organizzativo (tramite la FRIA). Se un deployer modifica in modo significativo il sistema o lo utilizza sotto il proprio nome o marchio, assume le responsabilità del fornitore.

Entrambi sono tenuti alla cooperazione reciproca e con le autorità: il fornitore fornisce supporto tecnico e adeguata documentazione, mentre il deployer segnala eventuali incidenti o usi impropri e rispetta istruzioni e limiti d'impiego.

1.4 Pratiche di IA vietate nel contesto di utilizzo

Con riferimento alle funzionalità del sistema di videosorveglianza, di lettura automatizzata delle targhe e di fototrappole intelligenti, si precisa che, ai sensi dell'art. 5 dell'AI Act, non sono previste né consentite le seguenti tipologie di utilizzo di sistemi di intelligenza artificiale:

a) **Valutazioni o previsioni del rischio criminale riferite a persone fisiche**, basate esclusivamente su attività di profilazione automatizzata o sull'analisi di tratti della personalità, comportamentali o caratteriali. Il sistema non è destinato a effettuare forme di *predictive policing* o di classificazione del rischio individuale. L'eventuale utilizzo dei dati raccolti avviene unicamente a supporto di valutazioni umane fondate su elementi fattuali, oggettivi e verificabili, direttamente connessi a eventi o condotte già occorse.

b) **Creazione o ampliamento di banche dati biometriche**, e in particolare di archivi di riconoscimento facciale, mediante raccolta indiscriminata di immagini provenienti da internet, social media o flussi video di telecamere. L'impianto non prevede funzioni di riconoscimento facciale né l'estrazione sistematica di immagini biometriche a fini identificativi.

c) **Inferenza o analisi delle emozioni delle persone fisiche**, sia in contesti lavorativi sia in contesti assimilabili a quelli educativi. Il sistema non è progettato per rilevare, dedurre o interpretare stati emotivi, intenzioni o condizioni psicologiche degli interessati, né per finalità di controllo comportamentale.

d) **Categorizzazione biometrica delle persone fisiche**, finalizzata a trarre deduzioni o inferenze relative a caratteristiche particolarmente sensibili quali razza o origine etnica, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale. L'impianto non effettua alcuna forma di classificazione individuale basata su dati biometrici, né utilizza tali dati per finalità discriminatorie o di profilazione avanzata.

e) **Identificazione biometrica remota in tempo reale**, per la quale il Regolamento prevede specifiche e rigorose restrizioni. L'impianto di videosorveglianza e le tecnologie accessorie adottate non consentono l'identificazione biometrica automatizzata in tempo reale delle persone fisiche, né l'incrocio dei flussi video con banche dati biometriche a fini identificativi.

2. ELEMENTI PER LA CLASSIFICAZIONE DEL LIVELLO DI RISCHIO DEL SISTEMA DI IA

2.1. Sistemi ad alto rischio

2.1.1 Sono considerati ad alto rischio: (allegato III Ai Act per quanto applicabile al contesto)

a) **Sistemi di IA impiegati per la valutazione dell'affidabilità degli elementi probatori** nell'ambito di indagini o procedimenti penali. Le tecnologie adottate non svolgono alcuna funzione di analisi, ponderazione o validazione automatizzata delle prove, limitandosi alla mera acquisizione e registrazione di immagini o dati oggettivi, la cui valutazione resta integralmente demandata all'intervento umano delle autorità competenti.

b) **Sistemi di IA utilizzati per determinare o prevedere il rischio di commissione di reati o di recidiva**, anche quando tali valutazioni non si fondino esclusivamente sulla profilazione ai sensi dell'art. 3, par. 4, della direttiva (UE) 2016/680, ma includano l'analisi di tratti della personalità, comportamenti individuali o precedenti penali. L'impianto non è destinato a effettuare valutazioni predittive, scoring di rischio o classificazioni individuali delle persone fisiche.

c) **Sistemi di IA finalizzati alla profilazione delle persone fisiche** nel contesto delle attività di indagine, accertamento o perseguimento dei reati, ai sensi dell'art. 3, par. 4, della direttiva (UE) 2016/680. Le funzionalità implementate non consentono né supportano attività di profilazione automatizzata, analisi comportamentale avanzata o costruzione di profili individuali o di gruppo.

2.1.2 I sistemi non sono considerati ad alto rischio se non presentano un rischio significativo di:

d) danno per la salute;

e) sicurezza;

f) lesione dei diritti fondamentali delle persone fisiche;

g) influenza sul processo decisionale (non deve influenzare materialmente il risultato del processo decisionale);

h) profilazione di persone fisiche (un sistema di IA di cui al punto 2.1.2 (allegato III Ai Act) è sempre considerato ad alto rischio qualora esso effettui profilazione di persone fisiche. Tenuto conto che per profilazione si intende la definizione del Reg. UE 2016/679 supportato dalle linee guida WP 251 rev.01).

3. DESCRIZIONE DELLE TECNOLOGIE E DELLE FUNZIONALITÀ

3.1 Videosorveglianza per la sicurezza urbana

a) Telecamere fisse e orientabili in punti strategici (es. vie principali, piazze, luoghi soggetti a vandalismo).
b) Possibilità di analisi intelligente dei flussi video in tempo reale
c) Descrizione del prodotto di AI "VideoAnalisi LIVE"

Tecnologia utilizzata: iSentry Core
Nome del prodotto: VideoAnalisi LIVE
Hardware necessario: Server dedicato installato presso il Comune di Mirandola

d) Descrizione di "VideoAnalisi LIVE su tecnologia iSentry" (di seguito solo VideoAnalisi Live)

Il sistema VideoAnalisi LIVE è una soluzione di videoanalisi automatizzata basata su intelligenza artificiale, progettata per rilevare in tempo reale comportamenti anomali o potenzialmente critici all'interno di ambienti video sorvegliati, come spazi pubblici, aree aziendali o infrastrutture sensibili.
L'obiettivo principale del sistema è supportare gli operatori umani nella sorveglianza, fornendo segnalazioni (alert) mirate che evidenziano eventi ritenuti inusuali o meritevoli di attenzione. Questi eventi possono riguardare, ad esempio:

- movimenti improvvisi o sospetti in aree riservate;
- oggetti lasciati incustoditi;
- attraversamenti non autorizzati;
- comportamenti che si discostano dal normale flusso delle persone o dei veicoli.

Il funzionamento di VideoAnalisi LIVE si basa su un processo di osservazione automatica e continua delle immagini video, senza tuttavia effettuare identificazione o riconoscimento delle persone. Il sistema non acquisisce, elabora o conserva dati biometrici o identificativi, ma si limita ad analizzare schemi di movimento e modelli visivi attraverso l'interpretazione di pixel e gruppi di pixel.

Gli algoritmi di rilevamento e classificazione si basano su reti neurali pre-addestrate con dati generici e sintetici, utilizzati esclusivamente in fase di sviluppo. Durante il normale funzionamento, non avviene alcun apprendimento continuo e il sistema non modifica il proprio comportamento sulla base dei dati osservati. Ciò garantisce che l'intelligenza artificiale operi in modo statico, senza rischi di evoluzione incontrollata o adattamento imprevisto.

La generazione degli alert è soggetta a regole predefinite configurate nel sistema, che filtrano e selezionano le segnalazioni prima della visualizzazione. Le decisioni finali sul significato e sulla rilevanza dell'evento segnalato restano sempre in capo all'operatore umano, che ha il compito di valutare il contesto e decidere eventuali azioni successive.

VideoAnalisi LIVE è progettato per operare all'interno dell'ambiente locale del sistema di videosorveglianza, senza esportare dati verso l'esterno o comunicare con sistemi remoti. Non dispone di accessi cloud o di funzionalità di trasmissione remota, e tutte le comunicazioni interne si avvalgono di protocolli di sicurezza e cifratura.

In sintesi, VideoAnalisi LIVE:

- non effettua riconoscimento individuale;
- non raccoglie dati personali;
- non apprende dai dati osservati;
- non prende decisioni autonome;
- è soggetto a supervisione umana continua.

Tali caratteristiche concorrono a limitare significativamente i rischi per i diritti e le libertà fondamentali degli interessati, rendendo il sistema conforme ai principi dell'AI Act e, ove rilevante, compatibile con un utilizzo in scenari ad alto rischio con opportune misure di garanzia.

3.2 Tabella degli alert attivati dal Comune di Mirandola in VideoAnalisi LIVE

num	Funzionalità Alert (Unsupervised Self learning Unusual Behaviour)	La funzionalità è resa disponibile al Comune	Commenti	Informazioni aggiuntive	La funzionalità è attivata dal deployer
1	Comportamento anomalo Il sistema impara la condizione di movimento ordinaria e qualora la condizione sia inusuale / non ordinaria segnala con un alert. (Es. all'interno di una rotatoria dove avviene la circolazione antioraria degli autoveicoli, qualora avvenga un movimento in senso orario il sistema segnala un'anomalia) (Es. in una strada con i marciapiedi tutti attraversano sulle strisce, se alcuni non attraversano sulle strisce allora situazione anomala)	**SÌ (consente addestramento)**	Vedi specifico insolito comportamento documento per l'uso dettagliato delle applicazioni dei casi	È attivabile su specifiche telecamere a discrezione del deployer	**SI, la funzionalità è attivata sulle registrazioni**
	Analisi del movimento				
2	Filtro ambientale AI Riduzione degli errori (sempre attivato)	**SÌ**	Capacità di rilevare e tracciare bersagli	Utilizzabile in ambienti pubblici	**SI, la funzional**

			reali eliminando interferenze ambientali Utilizzato per affinare i risultati desiderati e ridurre gli errori di identificazione delle situazioni da segnalare		**ità è attivata sulle registrazioni**
3	Oggetti dimenticati o persi	**SÌ (consente addestramento)**	Rileva e classifica oggetti abbandonati nell'area inquadrata, o rimossi generando allarmi o avvisi per zone specifiche. La dimensione dell'oggetto e il tempo di permanenza o assenza degli oggetti sono configurabili per ogni zona.	all'aperto o al chiuso per rilevare abbandono di rifiuti od oggetti, rimozione o furto, intrusione in aree interdette.	**SI, la funzionalità è attivata sulle registrazioni**
4	Analitiche Tripwire avanzate	**SÌ (consente addestramento**	Il sistema rileva quando uno o più oggetti (auto, persone, camion ecc.) attraversano una linea virtuale in una direzione specifica e, in base a regole personalizzate (che possono includere anche il numero di oggetti rilevati), genera allarmi o avvisi.		**SI, la funzionalità è attivata sulle registrazioni**
	Ingresso non autorizzato in un perimetro definito o in un'area				
5	Avviso di minaccia imminente	**SÌ (consente**	Rileva obiettivi che si	Stabilite le aree	**NO**

		addestramento)	avvicinano ad aree critiche	critiche si possono impostare allarmi in caso di presenza di Movimento all'interno di esse.	
6	Rilevamento intrusione a corto raggio	**SÌ**	Alta precisione e bassa latenza acquisizione 0-70 metri	Le prestazioni sono garantite solo se la configurazione rispetta le best practice e le soglie specificate per campo visivo, dimensione oggetto, risoluzione e angolo	**NO**
7	Rilevamento intrusione a medio raggio	**SÌ**	Elevata precisione fino a 250 metri		**NO**
8	La telecamera PTZ può essere comandata per spostarsi automaticamente su una posizione predefinita	**SÌ**			**NO**
	Classificazione				
9	Classificazione e verifica degli oggetti	**SÌ**	Possibilità di classificare oltre 100 tipi di oggetti (es. persone, veicoli, animali, laptop ecc.). Non vengono raccolti dati biometrici. Il sistema è in grado di distinguere persone da veicoli, animali,	Le prestazioni sono garantite solo se la configurazione rispetta le best practice e le soglie Specificate per campo visivo, dimensione oggetto, risoluzione	**SI, la funzionalità è attivata sulle registrazioni**

			etc.		
10	Rilevamento fumo e fuoco	**SÌ**	Prestazioni garantite solo in conformità con le migliori pratiche di configurazione e specificate soglie per FoV, dimensione dell'oggetto, risoluzione, angolo e densità dei pixel (fare riferimento a specifiche documentazione)	e angolo.	**SI, la funzionalità è attivata sulle registrazioni**
	Altre funzioni di classificazione speciale				
11	Conteggio oggetti (PERSONE O VEICOLI) (entrata/uscita)	**SÌ**	Basato su più telecamere.		**SI, la funzionalità è attivata sulle registrazioni**
12	Conteggio oggetti in un area di occupazione predefinita (per telecamera)	**SÌ**	Basato su una singola telecamera		**SI, la funzionalità è attivata sulle registrazioni**
13	Monitoraggio densità e reportistica (per area)	**SÌ**	Monitoraggio densità e reportistica (per area)	(funziona solo se è attivo il conteggio persone).	**SI, la funzionalità è attivata sulle registrazioni**
14	Verifica conformità mascherine (persone fisiche)	**SÌ**			**NO**
15	Distanziamento sociale e analisi gruppi	**SÌ**	Prestazioni garantite solo con posizionamento conforme della		**SI, la funzionalità è attivata sulle**

			telecamera, distanza, risoluzione e densità di pixel.		**registrazioni**
16	Rilevamento gruppi e folle	**SÌ**			**SI,la funzionalità è attivata sulle registrazioni**
17	Rilevamento stazionamento di persone (programmabile) Es. persone che sostano in prossimità di aree critiche	**SÌ**			**SI, la funzionalità è attivata sulle registrazioni**
18	Verifica DPI e reportistica (programmabile)	**SÌ**			**NO**
19	Rilevamento di denaro contante	**SÌ**			**NO**
20	Mappe di calore Occupazione delle diverse zone da parte di persone Es. area maggiormente utilizzate dai pedoni per rilevare abitudini	**SÌ**	Basato su singola telecamera		**NO**
	Motore delle regole				
21	Elaborazione con configurazioni limitate	**SÌ**	Regole preconfigurate, applicabili per regione della scena	Consente di limitare l'azione del rilevamento in aree specifiche della scena ripresa; scelta limitata delle analitiche possibili.	**NO**
22	Elaborazione con configurazioni illimitate	**SÌ**	Regole personalizzate illimitate, applicabili per regione della scena.	Consente di limitare l'azione del rilevamento in aree specifiche della scena ripresa; scelta libera	**NO**

				delle analitiche possibili	
	Altre funzioni				
23	Reporting BI	**SÌ**	Reporting KPI sulla cronologia degli avvisi (per telecamera, per sito ecc.) e sull'efficienza dell'operatore	Report dettagliati sull'operatività del sistema	**NO**
24	Ricerca forense negli avvisi	**SÌ**	Consente di cercare oggetti classificati all'interno dei dati di avviso già acquisiti per telecamera.	Ricerca specifica nell'elenco avvisi	**SI, la funzionalità è attivata sulle registrazioni**
25	Rilevamento di gruppi e folle	**SÌ**		In specifiche condizioni (es telecamere con la giusta qualità e corretta installazione) è possibile eseguire un controllo di affollamento	**SI, la funzionalità è attivata sulle registrazioni**
26	Offuscamento volti per GDPR e anonimato	**SU RICHIESTA AL FORNITORE**	In condizioni specifiche e con configurazioni specifiche è possibile eseguire l'offuscamento automatico		**SI, la funzionalità è attivata sulle registrazioni**
27	Analisi del suono	**SU RICHIESTA AL FORNITORE**	Utilizza il microfono della telecamera per l'analisi dei suoni nell'ambiente, Per esempio per rilevare spari		**NO**
28	Registrazione di clip di allarme	**SÌ**	Possibilità di rivedere i video prima e dopo l'allarme		**NO**

29	Riconoscimento facciale	**SU RICHIESTA AL FORNITORE**			**NO**
30	Riconoscimento delle targhe	**SU RICHIESTA AL FORNITORE**			**SI, la funzionalità è attivata sulle registrazioni**

4. AMBITO APPLICATIVO E FINALITÀ

4.1 Il progetto

Il Comune di Mirandola, in qualità di deployer del sistema IA, ha provveduto ad integrare ausili informatici che si avvalgono di intelligenza artificiale nei sistemi di videosorveglianza, lettura targhe e fototrappole, finalizzati allo svolgimento delle funzioni istituzionali di tutela della sicurezza urbana, controllo del traffico ed eventuali indagini di polizia giudiziaria e attività di tipo sanzionatorio in caso di abbandono illegittimo dei rifiuti. L'implementazione dell'IA nei propri sistemi mira ad automatizzare attività semplici e ripetitive, liberando tempo di lavoro per attività a maggior valore, aumentare le capacità predittive, supportare la personalizzazione dei servizi incentrata sull'utente, aumentando l'efficacia, l'efficienza e la tempestività dei servizi, promuovere l'innovazione dei servizi pubblici e dei processi amministrativi.

4.2 Tabella di pianificazione e definizione dell'ambito applicativo e delle finalità

Descrizione e analisi del sistema IA	Quali sono gli obiettivi principali del sistema IA?	**a) prevenire e reprimere atti delittuosi, attività illecite ed episodi di microcriminalità commessi sul territorio comunale, al fine di garantire maggiore sicurezza ai cittadini;** **b) prevenire e reprimere ogni tipo di illecito, di natura penale o amministrativa, in particolare legato a fenomeni di degrado e svolgere i controlli volti ad accertare e sanzionare le violazioni delle norme contenute nel regolamento di polizia urbana, nei regolamenti locali in genere e nelle ordinanze sindacali;** **c) vigilare sull'integrità, sulla conservazione e sulla tutela del patrimonio pubblico e privato,** **d) tutelare l'ordine, il decoro e la quiete pubblica;** **e) controllare aree specifiche del territorio comunale;** **f) monitorare i flussi di traffico;** **g) verificare e calibrare il sistema di gestione centralizzata degli impianti semaforici** **h) Verificare circolazione senza assicurazione, o con revisione scaduta; ricerca automezzi oggetto di indagine (su incarico dell'AG)** **i) Contrastare e sanzionale l'abbandono abusivo dei rifiuti.**
	Quali sono le caratteristiche principali del sistema?	Il sistema IA è progettato per estrarre dati significativi da grandi quantità di materiale video, consentendo una rapida analisi e individuazione di

		eventi chiave (grazie a molteplici "filtri" abbinati ad altrettanti algoritmi). La tecnologia alla base comprende il riconoscimento di oggetti, il tracciamento del movimento, e l'analisi comportamentale, consentendo una valutazione approfondita delle registrazioni. Inoltre, il sistema integra funzionalità di ricerca avanzate, permettendo agli utenti di effettuare richieste specifiche come il riconoscimento di oggetti o movimenti.
	In quali paesi verrà utilizzato?	Italia. Limitatamente al territorio di competenza del Comune di Mirandola.
	Quali tipologie di dati vengono elaborati dal sistema (personali, non personali, categorie particolari)?	Dati personali: Immagini personali derivanti dalle inquadrature e/o dalle registrazioni che costituiscono identità fisica ex art. 4, comma 1, punto 1) del GDPR; Categorie particolari di dati: Nessuna Dati giudiziari: NO Tali dati vengono raccolti dalle inquadrature e registrazioni dalle videocamere
	Identificazione dei potenziali soggetti interessati: chi sono gli individui o i gruppi che potrebbero essere interessati dal sistema AI, compresi i soggetti o i gruppi vulnerabili?	Cittadini e/o comunque tutti i soggetti che vengono ripresi
	Identificazione dei soggetti responsabili: chi è coinvolto nella progettazione, nello sviluppo e nell'implementazione sistema IA? Qual è il loro ruolo?	a) Alma Sicurezza S.r.l. quale fornitore (provider) del sistema IA ha la responsabilità di garantire che il sistema soddisfi i requisiti essenziali di sicurezza, robustezza, qualità dei dati, documentazione e di eseguire i test di conformità, oltre a rilasciare la dichiarazione CE; b) Il Comune di Mirandola quale deployer del sistema IA deve vigilare sul funzionamento quotidiano dell'IA. Se il Comune modifica sostanzialmente il sistema può assumere il ruolo di fornitore (provider) per quella nuova versione con le conseguenti responsabilità.
Contesto dei	**Quali diritti**	Dopo aver analizzato tutti i diritti individuali, civili,

diritti fondamentali	**fondamentali sono potenzialmente interessati dall'uso del sistema IA?**	politici, economici e sociali sanciti dalla Carta dei diritti fondamentali dell'Unione Europea (CDFUE), dal Trattato sul Funzionamento dell'Unione Europea (TFUE) e dal Reg. UE 2016/679 (GDPR), nonché dai principi sanciti dalla Costituzione della Repubblica Italiana, si è concluso che i diritti potenzialmente interessati sono: - **Diritto alla protezione dei dati personali (Art. 8 Carta dei Diritti Fondamentali dell'UE, Art. 16 TFUE, Regolamento europeo sul trattamento dei dati (GDPR))** Motivazione: Una persona potrebbe essere monitorata mentre si trova in una zona pubblica. Il sistema raccoglie informazioni sul tempo che la persona trascorre vicino a determinati edifici o aree, sui suoi movimenti (ad esempio, entra in un negozio, una chiesa, un bar), e su altri comportamenti (ad esempio, fa una telefonata mentre cammina, incontra altre persone), la combinazione di questi dati potrebbe comunque portare all'identificazione della persona se i dati vengono incrociati con altre informazioni disponibili, come i movimenti registrati in altre telecamere o informazioni ottenute tramite dispositivi mobili. In questo caso, la riservatezza delle informazioni personali potrebbe essere compromessa, poiché i dati, pur non essendo direttamente identificabili in un primo momento, potrebbero essere utilizzati per ricostruire il comportamento e l'identità delle persone in modo indiretto, violando il principio di privacy e il diritto alla protezione dei dati. - **Diritto alla libertà e alla sicurezza (Art. 6 Carta dei Diritti Fondamentali dell'UE)** Motivazione: Le persone che attraversano una zona sorvegliata in tempo reale potrebbero alterare il loro comportamento per evitare di suscitare attenzione o essere fermate dagli operatori in caso di allarme. Ad esempio, se sanno che il sistema di AI segnala automaticamente qualsiasi comportamento sospetto, potrebbero evitare di sostare in luoghi pubblici, sentendosi limitati nel loro diritto a muoversi liberamente. - **Diritto alla libertà di espressione (Art. 11 Carta dei Diritti Fondamentali dell'UE)** Motivazione: in una zona pubblica, un gruppo di attivisti sta organizzando una manifestazione pacifica. Tuttavia, il sistema di videosorveglianza segnala automaticamente come "sospetto" ogni gruppo che si ferma insieme o che si raduna.

		Questo potrebbe disincentivare i partecipanti a riunirsi nuovamente e a parlare liberamente o a organizzare nuove proteste per paura di essere etichettati o segnalati ingiustamente, limitando la libertà di espressione. - **Diritto alla non discriminazione (Art. 21 Carta dei Diritti Fondamentali dell'UE)** Motivazione: Se l'algoritmo di intelligenza artificiale analizza il comportamento delle persone e genera alert basati su criteri come il colore della pelle, la provenienza etnica o altri fattori protetti, potrebbe generare discriminazioni. Ad esempio, se un algoritmo identifica come "comportamento sospetto" la presenza di persone con un determinato aspetto fisico o un gruppo etnico specifico, ciò potrebbe violare il diritto alla non discriminazione. - **Diritto alla protezione da trattamenti automatizzati (Art. 22 GDPR)** Motivazione: Se il sistema di AI segnala automaticamente che una persona sta “comportandosi in modo sospetto” basandosi su una serie di parametri (come il comportamento in una zona, il tempo trascorso in un determinato luogo, vicino ad una banca, ad un negozio di beni di lusso, ad un edificio pubblico). Se questa segnalazione automatizzata porta a un intervento da parte delle forze dell'ordine senza una revisione umana, la persona potrebbe trovarsi in una situazione in cui è sottoposta a controlli, violando così il diritto alla protezione da trattamenti automatizzati. - **Diritto alla protezione della famiglia e della vita privata (Art. 7 Carta dei Diritti Fondamentali dell'UE)** Motivazione: Se il sistema di videosorveglianza con AI sia installato in una piazza pubblica, ma che le telecamere non siano solo orientate verso le strade o le aree di passaggio, ma anche verso zone dove le persone si siedono o socializzano. In queste zone, la gente potrebbe sentirsi più a suo agio nel fare conversazioni private, utilizzare il telefono, o avere incontri informali, eventualmente al di fuori dell’ambito familiare, senza la preoccupazione di essere monitorata. Tuttavia, se il sistema raccoglie informazioni anche su questi comportamenti apparentemente privati, come la durata della conversazione, il tempo trascorso in una zona o l’interazione tra le persone, potrebbe invaso la loro vita privata.

	Quali strumenti giuridici nazionali/internazionali per la tutela dei diritti umani/fondamentali sono stati impiegati a livello operativo?	• Regolamento (UE) 2024/1689 (AI Act) e relative disposizioni sugli obblighi di trasparenza, supervisione umana e analisi dei rischi; • Regolamento (UE) 2016/679 (GDPR) e normative nazionali in materia di protezione dei dati personali e privacy; • Direttiva (UE) 2016/680 per la protezione delle persone fisiche riguardo al trattamento dei loro dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati e per l'esecuzione di sanzioni penali; • Linee guida WP 251 per la profilazione delle persone fisiche; • Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679 adottata dal 2 febbraio 2018 – Garante Privacy; • Provvedimento del Garante del 10 aprile 2025 in relazione all'utilizzo di sistemi AI (Artificial Intelligence) nella videosorveglianza; • Decreto-Legge 11 aprile 2025, n. 48 – "Disposizioni urgenti in materia di sicurezza pubblica, di tutela del personale in servizio, nonché di vittime dell'usura e di ordinamento penitenziario"; • D.P.C.M. 12 gennaio 2024, recante "Piano triennale per l'informatica nella pubblica amministrazione 2024-2026" sulla base del quale è garantita l'adozione di Linee Guida sulla raccolta e il trattamento di dati finalizzati all'utilizzo in sistemi AI; • Linee guida della Commissione Europea del 18 luglio 2025 "Linee guida sulla portata degli obblighi per i modelli di intelligenza artificiale di uso generale stabiliti dalla legge sull'intelligenza artificiale"; • Eventuali normative nazionali specifiche per i sistemi di videosorveglianza (decreti interni, provvedimenti del Garante Privacy).
Controlli in atto	**Quali politiche e procedure sono state poste in essere per valutare il potenziale impatto sui diritti fondamentali, compresa la partecipazione delle parti interessate?**	Non applicabile (N/D)
	È stata condotta, sviluppata e	È stata effettuata una valutazione d'impatto sulla protezione dei dati (DPIA) ed il produttore ha

	implementata una valutazione d'impatto su ambiti specifici (ad es. la protezione dei dati) o su determinate caratteristiche del sistema?	effettuato una valutazione d'impatto sui diritti fondamentali (FRIA) del sistema IA sviluppato.
Coinvolgimento degli stakeholder e due diligence	**Quali sono i principali gruppi o comunità potenzialmente influenzati dal sistema di IA?**	Cittadini e/o comunque tutti i soggetti che vengono ripresi
	Ci sono altri soggetti tenuti al controllo del sistema IA, oltre ai provider o deployer (ad es. autorità nazionali, agenzie governative)?	Agenzia per l'Italia digitale (AGID)
	Esistono partner commerciali, compresi service provider, che sono stati coinvolti nel processo di valutazione?	NO

5. CLASSIFICAZIONE DEL LIVELLO DEL RISCHIO

Deve essere stabilito se il sistema di IA rientra nei sistemi ad alto rischio.

Si rileva che l'eventuale attivazione di specifiche funzionalità di analisi o di generazione di alert, per loro natura potenzialmente incidenti sui diritti e sulle libertà fondamentali delle persone fisiche, potrebbe astrattamente determinare la qualificazione dell'intero sistema come sistema di IA ad alto rischio, con la conseguente applicazione integrale degli obblighi e degli adempimenti previsti dal Regolamento.

Tuttavia, ai fini di una valutazione sostanziale e proporzionata del rischio, appare necessario considerare non solo la configurazione teorica del sistema, ma anche la probabilità effettiva di utilizzo delle funzionalità riconducibili a scenari di alto rischio. Tale probabilità può essere valutata, in termini operativi, come frequenza e contesto di impiego delle predette funzionalità in situazioni che soddisfano i requisiti normativi dei sistemi ad alto rischio.

L'elaborazione di una scala di probabilità di utilizzo consente di stimare in modo più accurato il livello concreto di esposizione al rischio, permettendo di calibrare in maniera proporzionata le misure organizzative, tecniche e procedurali, nonché le garanzie di tutela dei diritti fondamentali, in funzione del reale grado di impiego del sistema di IA, ferma restando l'osservanza dei principi di legalità, necessità e proporzionalità.

5.1 Tabella per la determinazione del Rischio Alto (calcolo NRA e PRA)

Videosorveglianza per la sicurezza urbana con iSentry – VideoAnalisi LIVE

	Requisiti sistemi ad alto rischio sulla base della normativa (fornitori)	**SÌ/NO** **(Deployer)**	**Note** **(Deployer)**	**Probabilità di accadimento** **da 1 a 4** **0=non applicabile** **1=potenzialmente probabile,** **2=poco probabile,** **3=probabile,** **4=molto probabile**
1	a) sistemi di IA destinati a essere utilizzati dalle autorità di contrasto o per loro conto, oppure da istituzioni, organi e organismi dell'Unione a sostegno delle autorità di contrasto per valutare l'affidabilità degli elementi probatori nel corso delle indagini o del perseguimento di reati;	**SÌ**	Le autorità potrebbero richiedere tale attività	2 (poco probabile)
2	b) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto o per	**NO**		0 (non applicabile) non è possibile con la

	loro conto, oppure da istituzioni, organi e organismi dell'Unione a sostegno delle autorità di contrasto, per determinare il rischio di commissione del reato o di recidiva in relazione a una persona fisica non solo sulla base della profilazione delle persone fisiche di cui all'articolo 3, paragrafo 4, della direttiva (UE) 2016/680 o per valutare i tratti e le caratteristiche della personalità o il comportamento criminale pregresso di persone fisiche o gruppi;			tecnologia utilizzata
3	c) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto o per loro conto, oppure da istituzioni, organi e organismi dell'Unione a sostegno delle autorità di contrasto, per effettuare la profilazione delle persone fisiche di cui all'articolo 3, paragrafo 4, della direttiva (UE) 2016/680 nel corso dell'indagine, dell'accertamento e del perseguimento di reati.	**NO**		0 (non applicabile)
	I sistemi non sono considerati ad alto rischio se non presentano un rischio significativo di:			
4	danno per la salute,	**NO**	non applicabile al sistema fornito	0 (non applicabile)
5	la sicurezza	**NO**	non applicabile al sistema fornito	0 (non applicabile)
6	i diritti fondamentali delle persone fisiche,	**SÌ**	Per le funzioni attivate e per la circostanza che il sistema non agisce in	2 (poco probabile)

			modalità automatiche, è attivato e impostato da un operatore, sia per l'inizio della tipologia di attività da effettuare, sia per la conduzione dell'attività, che per la valutazione dell'esito dell'attività del sistema di AI. Anche qualora il sistema sia impostato per rilevare automaticamente eventi, la loro valutazione è a discrezione dell'operatore. È sempre l'operatore ad interpretare i risultati ed a coinvolgere un ulteriore persona fisica (es. il suo grado superiore) ad effettuare un ulteriore valutazione in merito alla veridicità prima di effettuare qualsiasi decisione che possa produrre degli effetti giuridici sulle persone (soggetti interessati)	
7	Libertà decisionale dell'operatore	**SÌ**	Il sistema può coadiuvare gli operatori al processo decisionale, ma non ha un'influenza diretta, né automatica, né materiale per produrre effetti decisionali o comunque giuridici.	2 (poco probabile)
8	Profilazione delle persone: un sistema di IA è sempre considerato ad alto rischio qualora esso effettui profilazione di persone fisiche.	**NO**	Il sistema non effettua Autonomamente e automaticamente la profilazione di persone fisiche, è utilizzato per ricerche ed eventi specifici, ma non costruisce profili di comportamento o abitudini. È utilizzato per verificare il	0 (non applicabile)

			posizionamento delle persone o degli autoveicoli in frame temporali diversi al fine di ricostruire il percorso effettuato.	
	STIMA APPROSSIMATIVA DELLA VALUTAZIONE IN MERITO ALLA PROBABLITA' MEDIA CHE IL SISTEMA POSSA RICADERE NEI SISTEMI AD ALTO RISCHIO			
	Considerato che è sufficiente che uno degli elementi di valutazione sia applicabile, e che ciò comporti la categorizzazione del sistema Ai ad "alto rischio", si procede a valutare la probabilità di accadimento di ogni singolo elemento, nonché della media complessiva.			
	È applicabile almeno uno dei requisiti che possono determinare un "rischio alto"	**Num di requisiti applicabili**	**Formula utilizzata**	**Probabilità media di rientrare nei requisiti ad "rischio alto"**
	SÌ	**NRA = Numero Requisiti Applicabili** **3 su 8** **(37,5%)**	Media della somma delle probabilità degli elementi applicabili	**PRA = Probabilità Rischio Alto** **2 (basso)**

5.2 Obblighi dei deployer (Comune di Mirandola) dei sistemi ad alto rischio (entro il 02 agosto 2026)

I deployer di sistemi di IA ad alto rischio:

a) adottano idonee misure tecniche e organizzative per garantire di utilizzare tali sistemi conformemente alle istruzioni per l'uso che accompagnano i sistemi.

b) affidano la sorveglianza umana a persone fisiche che dispongono della competenza, della formazione e dell'autorità necessarie, organizzando le proprie risorse ed attività al fine di attuare le misure di sorveglianza umana indicate dal fornitore

c) nell'effettuazione della sorveglianza umana afferente al controllo sui dati di input, il deployer garantisce che i dati di input siano pertinenti e sufficientemente rappresentativi alla luce della finalità prevista del sistema di IA ad alto rischio.

d) i deployer monitorano il funzionamento del sistema sulla base delle istruzioni per l'uso del fornitore e, se del caso, informano i fornitori su eventuali problematiche a tale riguardo (articolo 72 Ai Act), e:

d.1 Qualora abbiano motivo di ritenere che l'uso del sistema di IA in conformità delle istruzioni possa comportare un rischio che possa compromettere la conformità del prodotto (ai sensi dell'articolo 79, paragrafo 1), i deployer ne informano, senza indebito ritardo, il fornitore o il distributore e la pertinente autorità di vigilanza del mercato e sospendono l'uso di tale sistema.

d.2 Qualora abbiano individuato un incidente grave, i deployer ne informano immediatamente anche il fornitore, in primo luogo, e successivamente l'importatore o il distributore e le pertinenti autorità di vigilanza del mercato.

e) Conservano i log generati automaticamente dal sistema di IA ad alto rischio, nella misura in cui tali log sono sotto il loro controllo, per un periodo adeguato di almeno sei mesi (salvo diversamente disposto dal diritto dell'Unione o nazionale applicabile, in particolare dal diritto dell'Unione in materia di protezione dei dati personali).

f) Prima di mettere in servizio o utilizzare un sistema di IA ad alto rischio sul luogo di lavoro, i deployer che sono datori di lavoro informano i rappresentanti dei lavoratori e i lavoratori interessati che saranno soggetti all'uso del sistema di IA ad alto rischio (tali informazioni sono fornite, se del caso, conformemente alle norme e alle procedure stabilite dal diritto e dalle prassi dell'Unione e nazionali in materia di informazione dei lavoratori e dei loro rappresentanti).

g) I deployer di sistemi di IA ad alto rischio che sono autorità pubbliche o istituzioni, organi e organismi dell'Unione rispettano gli obblighi di registrazione presso la banca dati dell'UE dei sistemi ad alto rischio di cui all'allegato III Ai Act, istituita ai sensi dell'art. 71 Ai Act, in conformità all'articolo 49.

h) Ove accertino che il sistema di IA ad alto rischio che intendono utilizzare non è stato registrato nella banca dati dell'UE di cui all'articolo 71, non utilizzano tale sistema e ne informano il fornitore o il distributore.

i) DPIA: i deployer di sistemi di IA ad alto rischio usano le informazioni fornite a norma dell'articolo 13 del regolamento Ai Act (par. 2 punto 5 lettera f del presente documento) per adempiere al loro obbligo di effettuare una valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 del regolamento (UE) 2016/679 o dell'articolo 23 del D.Lgs. 51/2018.

j) Fatta salva la direttiva (UE) 2016/680, nel quadro di un'indagine per la ricerca mirata di una persona sospettata o condannata per aver commesso un reato, il deployer di un sistema di IA ad alto rischio per l'identificazione biometrica remota a posteriori chiede un'autorizzazione, ex ante o senza indebito ritardo ed entro 48 ore, da parte di un'autorità giudiziaria o amministrativa la cui decisione è vincolante e soggetta a controllo giurisdizionale, per l'uso di tale sistema, tranne quando è utilizzato per l'identificazione iniziale di un potenziale sospetto sulla base di fatti oggettivi e verificabili direttamente connessi al reato. Ogni uso è limitato a quanto strettamente necessario per le indagini su uno specifico reato.

k) Se l'autorizzazione richiesta a norma del primo comma è respinta, l'uso del sistema di identificazione biometrica remota a posteriori collegato a tale autorizzazione richiesta è interrotto con effetto immediato e i dati personali connessi all'uso del sistema di IA ad alto rischio per il quale è stata richiesta l'autorizzazione sono cancellati.

l) In nessun caso tale sistema di IA ad alto rischio per l'identificazione biometrica remota a posteriori è utilizzato a fini di contrasto in modo non mirato, senza alcun collegamento con un reato, un procedimento penale, una minaccia reale e attuale o reale e prevedibile di un reato o la ricerca di una determinata persona scomparsa.

m) Occorre garantire che nessuna decisione che produca effetti giuridici negativi su una persona possa essere presa dalle autorità di contrasto unicamente sulla base dell'output di tali sistemi di identificazione biometrica remota a posteriori.

n) Il presente paragrafo lascia impregiudicati l'articolo 9 del regolamento (UE) 2016/679 e l'articolo 10 della direttiva (UE) 2016/680 riguardo al trattamento dei dati biometrici.

o) Indipendentemente dalla finalità o dal deployer, ciascun uso di tali sistemi di IA ad alto rischio è documentato nel pertinente fascicolo di polizia e messo a disposizione della pertinente autorità di vigilanza del mercato e dell'autorità nazionale per la protezione dei dati, su richiesta, escludendo la divulgazione di dati operativi sensibili relativi alle attività di contrasto. Il presente comma lascia impregiudicati i poteri conferiti alle autorità di controllo dalla direttiva (UE) 2016/680.

p) I deployer presentano alle pertinenti autorità di vigilanza del mercato e alle autorità nazionali per la protezione dei dati relazioni annuali sul loro uso di sistemi di identificazione biometrica remota a posteriori, escludendo la divulgazione di dati operativi sensibili relativi alle attività di contrasto. Le relazioni possono essere aggregate per coprire più di un utilizzo.

q) Gli Stati membri possono introdurre, in conformità del diritto dell'Unione, disposizioni più restrittive sull'uso dei sistemi di identificazione biometrica remota a posteriori.

r) I deployer dei sistemi di IA ad alto rischio che adottano decisioni o assistono nell'adozione di decisioni che riguardano persone fisiche informano queste ultime che sono soggette all'uso del sistema di IA ad alto rischio. Per i sistemi di IA ad alto rischio utilizzati a fini di contrasto si applica l'articolo 13 della direttiva (UE) 2016/680 che prevede “l’esenzione” dell’informativa qualora tale informazione possa:

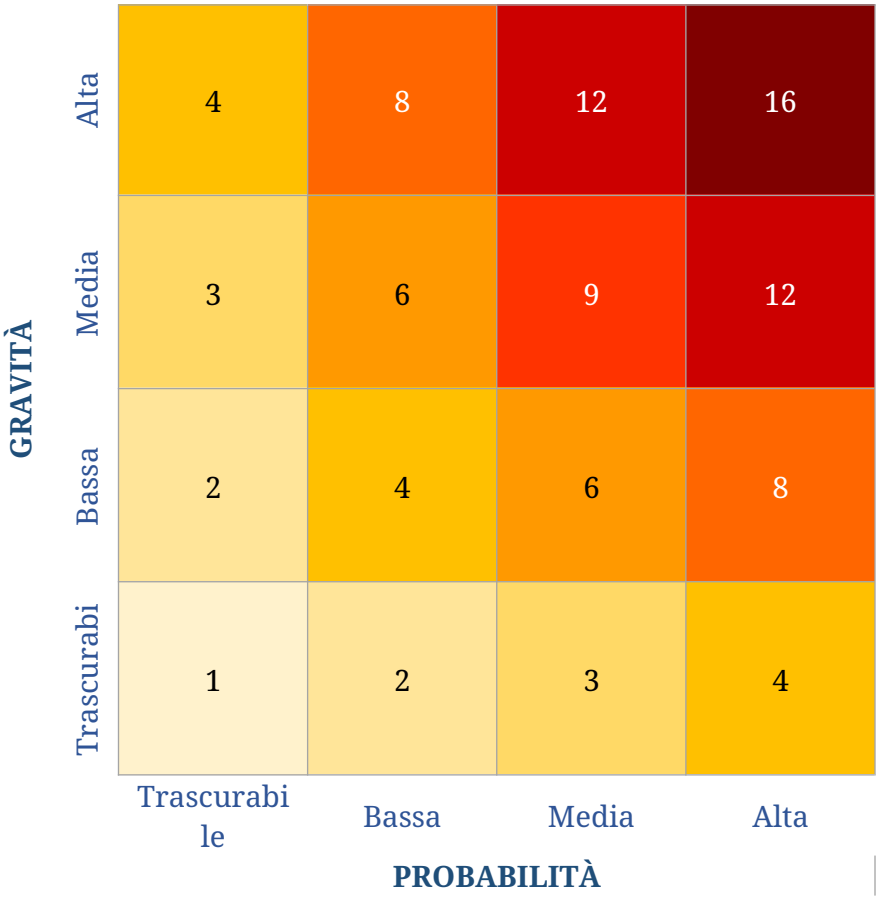
    r.1 compromettere indagini, inchieste o procedimenti ufficiali o giudiziari;

    r.2 compromettere la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali.

6. VALUTAZIONE DEL RISCHIO E DEGLI IMPATTI NEGATIVI NEL CONTESTO

6.1 Matrice probabilità, gravità, impatto

In questa sezione si classificano gli impatti, assegnando la probabilità di accadimento e la gravità.



Legenda
Gravità da 1 a 4:
(intensità del danno sui diritti e libertà delle persone)

0=non applicabile,
1=trascurabile,
2=basso,
3=medio,
4=alto

Probabilità di accadimento da 1 a 4:

0=non applicabile,
1=trascurabile (mai accaduto),
2=poco probabile,
3=probabile,
4=molto probabile

Potenziale impatto da 1 a 16:

Trascurabile (1) fino a <2
Basso (da 2 a 4) fino a <6
Medio (da 6 a 12) fino a <16
Alto (16)

6.2 Tabella di valutazione probabilità e gravità per l'impatto del danno sui diritti fondamentali (PI Base)

N	Diritti fondamentali descrizione	Applicabile / Non Applicabile (Eventuale commento)	Gravità da 1 a 4	Probabilità di accadimento da 1 a 4	Potenziale impatto (Gravità x Probabilità) Da 1 a 16
1	Diritto alla protezione dei dati personali (Art. 8 Carta dei Diritti Fondamentali dell'UE e Art. 16 TFUE): Il trattamento dei dati raccolti dal sistema di videosorveglianza (anche se non riguarda il riconoscimento facciale) è ricondotto alla definizione di "dato personale", ad esempio le immagini, i video, gli autoveicoli ed eventualmente se leggibile dalle immagini la targa, sono considerati dati personali, inoltre il trattamento potrebbe coinvolgere informazioni relative alla posizione e ai comportamenti delle persone. Oppure se le telecamere riprendono abitazioni private o loro porzioni, con un potenziale rischio per la riservatezza. L'intelligenza artificiale che analizza i movimenti	**SÌ** **Una persona potrebbe essere monitorata mentre si trova in una zona pubblica. Il sistema raccoglie informazioni sul tempo che la persona trascorre vicino a determinati edifici o aree, sui suoi movimenti (ad esempio, entra in un negozio, una chiesa, un bar), e su altri comportamenti (ad esempio, fa una telefonata mentre cammina, incontra altre persone), la combinazione di questi dati potrebbe comunque portare all'identificazione della persona se i dati vengono incrociati con altre informazioni disponibili, come i movimenti registrati in altre telecamere o informazioni ottenute tramite dispositivi mobili. In questo caso, la riservatezza delle informazioni personali potrebbe essere compromessa, poiché i dati, pur non essendo direttamente identificabili in un primo momento, potrebbero essere utilizzati per ricostruire il comportamento e**	**3 medio**	**2 poco probabile**	**6 medio**

	o altre caratteristiche comportamentali può essere vista come una forma di sorveglianza che impatta la privacy individuale.	**l'identità delle persone in modo indiretto, violando il principio di privacy e il diritto alla protezione dei dati.**			
2	Diritto alla libertà e alla sicurezza (Art. 6 Carta dei Diritti Fondamentali dell'UE): La sorveglianza in tempo reale può avere implicazioni sul diritto alla libertà di movimento e sicurezza, in quanto può influenzare il comportamento delle persone che sanno di essere monitorate. È importante considerare il rischio di una sorveglianza eccessiva o oppressiva che possa limitare la libertà personale, o comunque averne la parvenza.	**SÌ** Le persone che attraversano una zona sorvegliata potrebbero alterare il loro comportamento per evitare di suscitare attenzione o essere fermate dagli operatori in caso di allarme. Ad esempio, se sanno che il sistema di AI segnala automaticamente qualsiasi comportamento sospetto, potrebbero evitare di sostare in luoghi pubblici, sentendosi limitati nel loro diritto a muoversi liberamente.	**2 basso**	**2 poco probabile**	**4 basso**
3	Diritto alla libertà di espressione (Art. 11 Carta dei Diritti Fondamentali dell'UE): Un sistema di videosorveglianza che monitora costantemente le persone può influire sulla loro libertà di espressione, in quanto potrebbero sentirsi intimidite a interagire liberamente in uno spazio pubblico,	**SÌ** in una zona pubblica, un gruppo di attivisti sta organizzando una manifestazione pacifica. Tuttavia, il sistema di videosorveglianza segnala automaticamente come "sospetto" ogni gruppo che si ferma insieme o che si raduna. Questo potrebbe disincentivare i partecipanti a riunirsi nuovamente e a parlare liberamente o a organizzare nuove proteste per paura di essere	**3 medio**	**2 poco probabile**	**6 medio**

	sapendo di essere osservate.	etichettati o segnalati ingiustamente, limitando la libertà di espressione.			
4	Diritto alla non discriminazione (Art. 21 Carta dei Diritti Fondamentali dell'UE): L'intelligenza artificiale che analizza i comportamenti può introdurre rischi di discriminazione, ad esempio attraverso algoritmi che potrebbero rafforzare bias legati a età, etnia, genere o altre caratteristiche personali. È fondamentale valutare se il sistema potrebbe portare a trattamenti discriminatori.	**SÌ** Se l'algoritmo di intelligenza artificiale analizza il comportamento delle persone e genera alert basati su criteri come il colore della pelle, la provenienza etnica o altri fattori protetti, potrebbe generare discriminazioni. Ad esempio, se un algoritmo identifica come "comportamento sospetto" la presenza di persone con un determinato aspetto fisico o un gruppo etnico specifico, ciò potrebbe violare il diritto alla non discriminazione.	**1 trascurabile**	**1 trascurabile**	**1 trascurabile**
5	Diritto alla protezione da trattamenti automatizzati (Art. 22 GDPR): Se l'intelligenza artificiale produce decisioni automatizzate (come la generazione di alert senza intervento umano), è essenziale garantire che non vengano violati i diritti di protezione dalla profilazione o dalla decisione basata solo su trattamenti automatizzati, in particolare se tali decisioni influiscono significativamente	**SÌ** Se il sistema di AI segnali automaticamente che una persona sta “comportandosi in modo sospetto” basandosi su una serie di parametri (come il comportamento in una zona, il tempo trascorso in un determinato luogo, vicino ad una banca, ad un negozio di beni di lusso, ad un edificio pubblico). Se questa segnalazione automatizzata porta a un intervento da parte delle forze dell'ordine senza una revisione umana, la persona potrebbe trovarsi in una situazione in cui è sottoposta a controlli, violando così il diritto alla protezione da trattamenti automatizzati.	**1 trascurabile**	**1 trascurabile**	**1 trascurabile**

	sugli individui.				
6	Diritto a un giusto processo (Art. 47 Carta dei Diritti Fondamentali dell'UE): In caso di errore nell'identificazione o nel monitoraggio dei comportamenti, le persone potrebbero trovarsi in situazioni in cui l'alert prodotto dal sistema AI porta a conseguenze legali o amministrative. È importante assicurarsi che esistano meccanismi di ricorso e revisione.	**NO** Se un sistema AI segnali una persona come sospetta per essere stata in una zona durante un determinato orario, e queste informazioni vengano utilizzate come prova in un processo. Se l'algoritmo non ha una comprensione completa del contesto (ad esempio, la persona stava semplicemente aspettando un amico in una zona pubblica e non stava commettendo alcun reato), potrebbe contribuire erroneamente a una decisione giuridica. Il rischio qui è che la persona venga giudicata ingiustamente basandosi su una ricostruzione automatizzata di eventi che potrebbe non essere accurata o giuridicamente valida.	**1 trascurabile**	**1 trascurabile**	**1 trascurabile**
7	Diritto alla protezione della famiglia e della vita privata (Art. 7 Carta dei Diritti Fondamentali dell'UE): La videosorveglianza potrebbe comportare la registrazione o la sorveglianza di persone in situazioni private o semi-private. La gestione di tale monitoraggio deve rispettare i limiti necessari e proporzionati rispetto agli scopi	**SÌ** Se il sistema di videosorveglianza con AI sia installato in una piazza pubblica, ma che le telecamere non siano solo orientate verso le strade o le aree di passaggio, ma anche verso zone dove le persone si siedono o socializzano. In queste zone, la gente potrebbe sentirsi più a suo agio nel fare conversazioni private, utilizzare il telefono, o avere incontri informali, eventualmente al di fuori dell'ambito familiare, senza la preoccupazione di essere	**0 non applicabile**	**0 non applicabile**	**0 non applicabile**

	previsti, garantendo la protezione della sfera privata.	monitorata. Tuttavia, se il sistema raccoglie informazioni anche su questi comportamenti apparentemente privati, come la durata della conversazione, il tempo trascorso in una zona o l'interazione tra le persone, potrebbe invaso la loro vita privata.			
	VALUTAZIONE MEDIA DEL POTENZIALE IMPATTO DI BASE SUI DIRITTI E LIBERTA' DELLE PERSONE PRIMA DELL'APPLICAZIONE DELLE MISURE DI MITIGAZIONE				
	PI Base = Potenziale Impatto di base somma dei potenziali impatti / (numero di elementi che hanno rischio >0) : **PI Base = 19 / 6 = 3,1 (basso)**				

6.3 Indice di Monitoraggio Territoriale (IMT)

L'Indicatore di Intensità del Monitoraggio Territoriale (IMT) costituisce un fattore di correzione volto a normalizzare e ponderare una pluralità di variabili rilevanti ai fini della valutazione del rischio, tra cui, a titolo esemplificativo, l'estensione dell'area monitorata, la presenza di siti sensibili, il numero delle telecamere installate e le relative modalità di utilizzo, nonché la densità e le caratteristiche della popolazione interessata.

L'IMT consente di esprimere in termini sintetici il grado di estensione, frequenza e focalizzazione del monitoraggio effettuato mediante sistemi di intelligenza artificiale sul territorio, restituendo una misura proporzionale all'effettiva intensità dell'attività di osservazione L'indicatore incorpora un fattore di correzione dinamico, idoneo ad attenuare o, al contrario, ad amplificare l'impatto del monitoraggio sull'indice complessivo, fino a un massimo pari al raddoppio del valore di riferimento, in funzione delle specifiche condizioni operative e contestuali.
Tale fattore di correzione consente di incrementare o ridurre la gravità del rischio, intesa come intensità potenziale del pregiudizio ai diritti e alle libertà fondamentali delle persone fisiche, assicurando una valutazione graduata, coerente con i principi di proporzionalità e minimizzazione e idonea a riflettere il concreto livello di incidenza del sistema sul contesto territoriale di riferimento.

Ai fini della presente FRIA viene individuato l'indice di monitoraggio territoriale fornito (IMT) fornito dal produttore (provider) e calcolato mediante il foglio di calcolo allegato alla FRIA del produttore stesso, che riporta il valore **IMT = 1,46**

6.4 Calcolo del Potenziale Impatto sul Territorio

Il Potenziale Impatto sul Territorio (PIT) può essere calcolato utilizzando la formula:

PIT = PI Base × IMT

Dove:

- PI Base (Potenziale Impatto di Base) è la misura del potenziale impatto iniziale, che è il risultato della precedente tabella, varia su una scala da 1 a 16 (derivante dalla matrice 4x4, dove 16 rappresenta il massimo impatto).
- IMT (Indice di Monitoraggio Territoriale) è un fattore correttivo che tiene conto delle caratteristiche specifiche del territorio e dei suoi elementi di vulnerabilità, come la densità di popolazione, il numero di telecamera, le infrastrutture critiche, e la frequenza di monitoraggio.

Passaggi per il calcolo:

1. PI Base (calcolato al par. 6.2) = 3,1
2. IMT (fornito dal produttore): 1,46
3. Moltiplicare PI Base per IMT: Il risultato sarà il PIT, che rappresenta il potenziale impatto complessivo sul territorio, tenendo conto delle specificità e della capacità di monitoraggio sul territorio.

Se il PI Base è 3,1 (basso) su una scala da 1 a 16 (vedi matrice al par. 6.1), e l'IMT per quella zona specifica è 1,46 (indice che riflette un medio/alto livello di monitoraggio del territorio), il PIT sarà:

PIT = PI Base × IMT

PIT = 3.1 × 1.46 = 4.52 (medio)

In questo esempio, il PIT risulta essere 4,52, indicando un impatto medio rispetto al “PI Base” di partenza che era 3.1 (basso)

Poiché il Fornitore con la FRIA dallo stesso predisposta, ha individuato i possibili impatti sui diritti fondamentali derivanti dall’uso della tecnologia, il Comune, anche con riguardo allo scenario locale e al contesto territoriale nei quali sono svolte le attività di video analisi, definisce in modo specifico gli impatti sulla base delle funzioni affettivamente attivate e utilizzate.

7. MISURE DI MITIGAZIONE E GARANZIE

7.1 Trasparenza e informazione

a. Cartellonistica chiara con richiamo a informativa AI estesa nella quale è specificato che la videosorveglianza utilizza sistemi di IA", comunicazioni alla cittadinanza, pubblicazione di regolamenti comunali.
b. I sistemi di videoanalisi devono essere spiegabili: gli utenti devono poter comprendere come funzionano.

7.2 Controlli umani nei processi decisionali automatizzati

a. Prima di emettere sanzioni o segnalazioni, l'allarme del sistema deve essere validato da almeno un operatore umano formato.
b. Dev essere sempre mantenuta come centrale e imprescindibile la decisione che conferma o annulla un alert al fine del rispetto del principio "human-in-the-loop".
c. Definizione dei i protocolli di intervento, forma il personale all'utilizzo.

7.3 Limitazione del monitoraggio

a. Istruzioni al personale per la conservazione delle registrazioni video per il periodo massimo di giorni 7 per le estrazioni.
b. Limitazione degli alert attivati, e utilizzo solo per reali necessità di servizio, no finalità statistiche.

Reclamo

Deve essere prevista la possibilità e un meccanismo di reclamo e trasparenza per gli utenti.
Documentati: tutte le scelte progettuali, i dataset e gli esiti della valutazione devono essere tracciabili.

7.4 Misure di sicurezza

Proporzionalità:

Tutte le misure devono essere proporzionate al rischio identificato e tecnicamente implementabili

a) I sistemi, le apparecchiature ed il software devono rispondere alle misure di sicurezza tecniche ed organizzative di cui all'art. 32 del Reg. UE 2016/679, ed alle misure definite nella DPIA – valutazione di impatto ai sensi dell'art. 35 del Reg. UE 2016/679. Le misure di sicurezza definite nella DPIA si intendono parte integrante di questa valutazione. Le misure devono includere:
   - la pseudonimizzazione (ove necessario) e la cifratura dei dati personali;
   - la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
   - la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

b) Devono essere garantite le misure di sicurezza derivanti dall'art. 15 del Ai Act. La tabella al par. 8 punto 4 costituisce l'elenco di tali misure di sicurezza Ai Act.

7.5 Formazione (Alfabetizzazione in materia di IA – art. 4 AI ACT)

I fornitori e i deployer dei sistemi di IA adottano misure per garantire nella misura del possibile un livello sufficiente di alfabetizzazione in materia di IA del loro personale nonché di qualsiasi altra persona che si occupa del funzionamento e dell'utilizzo dei sistemi di IA per loro conto, prendendo in considerazione le loro conoscenze tecniche, la loro esperienza, istruzione e formazione, nonché il contesto in cui i sistemi di IA devono essere utilizzati, e tenendo conto delle persone o dei gruppi di persone su cui i sistemi di IA devono essere utilizzati.

L'intensità e il contenuto degli interventi formativi devono essere calibrati in funzione delle competenze tecniche, dell'esperienza pregressa, del grado di istruzione e del livello di formazione dei destinatari, nonché del contesto applicativo dei sistemi di IA e delle potenziali ricadute sul piano individuale e sociale derivanti dal loro utilizzo.

Il Regolamento non prescrive contenuti o modalità specifiche per l'erogazione delle attività formative in materia di intelligenza artificiale. L'impostazione dei programmi di alfabetizzazione dipende pertanto dal contesto organizzativo e dall'effettivo impiego dei sistemi di IA.

Nel documento di domande e risposte aggiornato al 8/7/2025 "Alfabetizzazione AI - Domande & Risposte", la Commissione Europea ha delineato i requisiti minimi che un percorso di "AI literacy" deve soddisfare per essere conforme al Regolamento. In particolare, è necessario assicurare una comprensione generale dell'intelligenza artificiale all'interno dell'organizzazione, in relazione al ruolo ricoperto e al livello di rischio associato ai sistemi impiegati. Le attività formative devono pertanto essere strutturate in base a questi elementi, tenendo conto delle competenze pregresse dei destinatari e del contesto applicativo.

La Commissione raccomanda inoltre di includere moduli dedicati alla comprensione del quadro giuridico, in particolare del Regolamento IA, nonché ai principi etici e di governance.

È necessario adottare percorsi differenziati per ruoli o livelli di responsabilità. Le organizzazioni non sono tenute a rilasciare certificazioni formali per la formazione, ma devono documentare internamente le iniziative svolte, attraverso un registro interno delle attività formative.

Ai sensi dell'art. 113 del Regolamento (UE) 2024/1689, la formazione disciplinata dal Capo I, art. 4 del Regolamento è obbligatoria a partire dal 02 febbraio 2025.

Il Comune di Mirandola adempie all'obbligo formativo individuando Funzioni, Ruoli e Livelli di formazione come segue:

Ruoli che utilizzano	Funzione all'interno dell'organizzazione	Livello di formazione

tecnologie di IA		
Ruoli decisionali e organizzativi	Es. Comandante	Livello base AI Livello organizzativo AI
Ruoli operativi	Es. Agente e altri soggetti incaricati	Livello base AI

Livello di formazione	Nome corso
Livello base AI	Cos'è (e cosa non è) un sistema AI - Interazione uomo- macchina - Diritti dei cittadini e regole da seguire - Cybersecurity e protezione dei dati - Simulazioni e casi pratici - Modalità didattiche
Livello organizzativo AI	Fondamenti strategici sull'IA - Risk governance e responsabilità - AI ad alto rischio nella PA - Etica, diritti e impatto sociale - Indicatori di efficacia e monitoraggio, requisiti e audit sui fornitori - Modalità didattiche

7.7 Efficacia delle misure di mitigazione sul Potenziale Impatto Totale

N	Misure di mitigazione	Note	Efficacia (1 – 4)
1	Trasparenza e informazione	Cartellonistica chiara, informativa estesa AI, comunicazioni e pubblicazione regolamenti. Riduce rischio di percezione negativa e aumenta fiducia pubblica.	3
2	Supervisione umana	Validazione obbligatoria di ogni alert da parte di un operatore formato, con audit trail delle decisioni. Elimina rischio decisioni automatizzate errate.	4
3	Limitazione del monitoraggio	Conservazione minima (<7 giorni), limitazione alert solo a necessità di servizio. Minimizza esposizione dati e riduce monitoraggio superfluo.	4
4	Misure di sicurezza	Pseudonimizzazione, cifratura, resilienza e continuità, test regolari. Riduce rischio di violazioni e garantisce protezione costante. Utilizzo check list di controllo.	4
5	Valutazione periodica e aggiornamento algoritmi	Monitoraggio falsi positivi/negativi, aggiornamenti software e protocolli di test. Migliora accuratezza e riduce bias.	3
6	Formazione AI literacy	Percorsi formativi di|erenziati per ruoli, conoscenza regolamentare e rischi AI. E|etto indiretto ma fondamentale a lungo	3

		termine.	
		Somma dell'efficacia (da 1 a 4) per ciascuna misura:	**21**

CALCOLO DELL'IMPATTO RESIDUO		
IMC = Indice di Mitigazione Complessivo 1- (somma efficacia / 24)	**PIT = Potenziale Impatto Totale** prima dell'adozione delle misure di mitigazione	**IR = Impatto Residuo** dopo l'applicazione delle misure di mitigazione **IR = IMC x PIT**
0,125	**4,52 (medio)**	**0,57 (trascurabile)**

8. MONITORAGGIO, AUDIT E REVISIONE CONTINUA

8.1 Sistema di log e tracciamento

a) Registrazione di chi accede alle immagini, chi inserisce, modifica o attiva i filtri, emette azioni sulla base degli alert, chi modifica in generale la configurazione del sistema.
b) Sono registrati anche i log degli ADS interni ed esterni (il fornitore o altri eventuali sub-fornitori per le attività di assistenza)

8.2 Audit interno ed esterno

a) Possibilità di controlli, audit, pareri da parte del RPD (Responsabile per la protezione dei dati).
b) Eventuali controlli da parte delle autorità di vigilanza (Garante Privacy, ACN, Agid).

8.3 Aggiornamento della FRIA

c) La FRIA deve essere aggiornata in caso di modifiche (nuovi algoritmi, alert, ampliamento dell'area di videosorveglianza, ecc.) e deve essere revisionata almeno 1 volta all'anno.

8.4 Check-list per verifica e aggiornamento delle misure di sicurezza

a) Le misure di "Accuratezza, robustezza e cybersicurezza" di cui all'art. 15 Ai Act sono verificate e revisionate con l'aggiornamento della presente FRIA.
b) Il Comune svolgerà le attività sottoindicate:

Check-list per verifica e aggiornamento delle misure di sicurezza

N	Misura	Descrizione operativa	Stato di attuazione SI / NO / note
1	Gestione continua del rischio Art. 9 (via Art. 29, par. 1)	Rivedere annualmente la FRIA e aggiornarla subito in caso di modifiche, incidenti o nuovi rischi.	SÌ
2	Controllo degli accessi fisici e logici Art. 15 + Art. 29, par. 4	Limitare l'accesso al sistema a personale autorizzato tramite chiavi, badge o credenziali.	SÌ
3	Autenticazione forte degli operatori Art. 15 + Art. 29, par. 4	Usare password complesse, e autenticazione a due fattori per accedere al sistema.	SÌ
4	Crittografia dei dati in transito e a riposo Art. 15 + Art. 10, par. 5	Proteggere i dati con cifratura durante la trasmissione e l'archiviazione.	SÌ
5	Segmentazione e isolamento di rete Art. 15	Separare la rete del sistema IA da altre reti aziendali per ridurre rischi di intrusione.	SÌ

6	Backup e ripristino con test periodici Art. 15	Eseguire copie di sicurezza dei dati e testarne il ripristino almeno una volta l'anno.	SÌ
7	Aggiornamenti di sicurezza del costruttore / fornitore sia per l'hardware che per il software Art. 15	Applicare regolarmente aggiornamenti di sicurezza e configurazioni protettive di hw e sw.	SÌ
8	Monitoraggio continuo di sicurezza Art. 15 + Art. 72	Usare strumenti per rilevare intrusioni, anomalie o accessi sospetti in tempo reale.	NO
9	Supervisione umana efficace Art. 14 + Art. 29, par. 1	Garantire che un operatore verifichi e validi sempre le segnalazioni del sistema.	SÌ
10	Possibilità di arresto o disattivazione immediata Art. 14	Assicurarsi che esista un comando o procedura per fermare subito il sistema e che sia efficace.	SÌ
11	Validazione umana degli alert Art. 14 + Art. 29, par. 1	Registrare chi ha preso decisioni sugli alert e le azioni eseguite.	SÌ
12	Logging delle decisioni operative Art. 12 + Art. 29, par. 4	Registrare chi ha preso decisioni sugli alert e le azioni eseguite.	SÌ
13	Minimizzazione dei dati raccolti Art. 10, par. 5 + Art. 29, par. 3	Configurare il sistema per acquisire solo i dati strettamente necessari.	SÌ
14	Pseudonimizzazione o mascheramento dei dati Art. 10, par. 5	Offuscare e rendere non identificabili direttamente i dati personali dove possibile, tenuto conto che l'offuscamento in generale non è una misura che garantisce l'anonimizzazione.	SÌ
15	Limitazione dei tempi di conservazione Art. 10, par. 5 + Art. 29, par. 3	Cancellare ogni ripresa o informazione se non più necessaria entro 7 giorni dall'acquisizione, anche prima se non necessaria, salvo disposizioni dell'AG per indagini in corso.	SÌ
16	Cancellazione sicura dei dati Art. 10, par. 5 + Art. 29, par. 3	Eliminare i dati in modo irreversibile secondo procedure sicure.	SÌ
17	Audit periodici di configurazione e privacy Art. 29, par. 5 + Art. 72	Controllare almeno annualmente impostazioni e misure tecniche di cui all'art. 32 del GDPR.	SÌ
18	Test periodici di accuratezza e performance Art. 15 + Art. 29, par. 5	Misurare regolarmente il tasso di falsi positivi/negativi e prestazioni attraverso la compilazione del registro.	NO
19	Protezione da attacchi adversariali (manipolazione dei dati in ingresso) Art. 15	Adottare filtri e controlli per ridurre il rischio di manipolazioni dati in input. Verificare i dati che provengono dalle telecamere al sistema di Ai, no distorti o anomali (es. controllo qualità	SÌ

		immagini)	
20	Controllo di integrità dei dati Art. 15 + Art. 10	Verificare che i dati non siano stati alterati o corrotti.	SÌ
21	Procedura di segnalazione degli incidenti Art. 73 + Art. 29, par. 6	Stabilire un canale ed una procedura per notificare guasti o violazioni.	SÌ
22	Registro e analisi degli incidenti Art. 72 + Art. 73	Annotare tutti gli incidenti sul registro e analizzarli per evitare che si ripetano.	SÌ
23	Simulazioni di gestione incidenti Art. 15 + Art. 72	Organizzare almeno un test di risposta simulando un incidente di sicurezza.	NO
24	Formazione continua degli operatori Art. 29, par. 5	Adozione della procedura di formazione	SÌ
25	Aggiornamenti formativi su modifiche tecnologiche e normative Art. 29, par. 5	Formare il personale quando cambiano sistema o norme.	SÌ
26	Sensibilizzazione etica e giuridica del personale Art. 29, par. 5	Spiegare le implicazioni giuridiche ed etiche dell'uso del sistema di AI.	SÌ

9. CONCLUSIONI E VALUTAZIONE FINALE

9.1 Bilanciamento tra sicurezza urbana e diritti fondamentali

Analisi dei requisiti per il rischio

Indice	Descrizione	Note	Valore
NRA %	**Numero Requisiti Applicabili %** Percentuale dei requisiti applicabili al sistema affinché sia suscettibile di essere categorizzato a "Rischio Alto"	Dall'analisi sono soddisfatti 3 requisiti su 8 per il rischio alto.	3 su 8 37,5%
PRA	**Probabilità Rischio Alto** Probabilità media di utilizzo del sistema che comportano un rischio elevato	Tuttavia la probabilità media di utilizzo funzionalità che riconducono ad un rischio alto è limitata	2 (basso)

FRIA - Freedom Right Impact Analysis – Valutazione di impatto sui diritti fondamentali			
PI Base	**Potenziale Impatto di base**	Impatto tenuto conto della probabilità e gravità di accadimento	**3,1 (basso)**
IMT	**Indice di Monitoraggio Territoriale**	Fattore di correzione su base territoriale e di monitoraggio	1,46
PIT	**Potenziale Impatto Totale**	Impatto tenuto conto del monitoraggio territoriale applicabile al contesto	**4,52 (medio)**
IMC	**Indice di Mitigazione Complessivo**	Grado di attenuazione dell'impatto a seguito dell'adozione delle misure di garanzia e sicurezza	0,125
IR	**Impatto Residuo** dopo l'applicazione delle misure di mitigazione **IR = IMC x PIT**	Impatto sui diritti fondamentali delle persone dopo l'applicazione delle misure di attenuazione	**0,57 (trascurabile)**

Con le misure di mitigazione previste, l'impatto di violazione dei diritti fondamentali è così valutato:

A seguito delle misure di mitigazione e di sicurezza implementate l'impatto residuo sui diritti fondamentali delle persone risulta trascurabile.

Mirandola (MO)

Comune di Mirandola

Il Sindaco