IL RUOLO DELL'INTELLIGENZA ARTIFICIALE TRA LE FORZE DELL'ORDINE. LA POLITICA DELLA DIFESA E IL DIRITTO ALLA PRIVACY*

di Fatoumata Diawara**

Sommario. 1. Introduzione: IA e razionalità tecnologico-securitaria. – 2. Il ruolo dell'intelligenza artificiale nelle forze dell'ordine. – 3. Bilanciare la sicurezza nazionale italiana e i diritti alla privacy nell'era dell'intelligenza artificiale. – 3.1. Il rapporto tra *AI Act*, GDPR e Codice *privacy*: un confronto sistematico. – 4. Il quadro giuridico europeo e le sue implicazioni. – 5. L'intelligenza artificiale nei contesti operativi internazionali. – 6. Considerazioni etiche nell'impiego dell'IA. – 7. Conclusione.

1. Introduzione: IA e razionalità tecnologico-securitaria. L'integrazione dell'intelligenza artificiale (IA) nei settori della sicurezza e della difesa pubblica rappresenta una delle trasformazioni più incisive nel panorama tecnologico e normativo globale. L'adozione di strumenti automatizzati, tra cui algoritmi predittivi e sistemi decisionali autonomi, solleva interrogativi cruciali sul bilanciamento tra efficienza operativa, legalità e tutela dei diritti fondamentali. In particolare, l'evoluzione da modelli *Human in the Loop* a configurazioni *Human on/out of the Loop*[1] evidenzia una crescente delega decisionale alle macchine, con significative implicazioni etiche e giuridiche, soprattutto in relazione ai principi di trasparenza e alla responsabilità delle scelte automatizzate. A livello europeo, il Regolamento sull'intelligenza artificiale (*AI Act*), approvato nel 2024, ha introdotto un sistema normativo fondato su un approccio basato sul rischio (*risk-based approach*)[2], che prevede obblighi di trasparenza algoritmica, tracciabilità dei processi decisionali, supervisione umana e valutazioni d'impatto per i sistemi ad alto rischio. Tuttavia, la sua attuazione nei contesti nazionali presenta ancora criticità rilevanti, sia sotto il profilo dell'armonizzazione normativa sia riguardo alla capacità istituzionale di garantire un controllo effettivo. Il caso italiano è emblematico: il disegno di legge sull'IA, oggetto del parere motivato della Commissione europea (C (2024) 7814), evidenzia divergenze rispetto al quadro comunitario, tra cui definizioni non conformi, obblighi eccessivi per alcune categorie professionali sensibili, carenze di indipendenza delle autorità di controllo (AgID e ACN) e sovrapposizioni normative in materia di *watermarking*[3]. Tali disallineamenti non solo compromettono la coerenza con l'*AI Act* e con il GDPR, ma rischiano di generare una frammentazione

* *Sottoposto a referaggio.*

** Dottoranda in Società in mutamento. Politiche, diritti e sicurezza – Università degli Studi della Tuscia.

[1] ISSMI – 25° Corso Superiore di Stato Maggiore Interforze, 1ª Sezione, 2° Gruppo di lavoro, *Applicazione di Artificial Intelligence per fini militari: individuazione dei criteri relativi al passaggio dall'approccio Human in the Loop allo Human on the Loop e definizione delle conseguenti implicazioni sul ciclo di definizione e approvazione delle ROE*, Centro Alti Studi per la Difesa – Istituto di Ricerca e Analisi della Difesa, Roma, 2023, spec. 22-28.

[2] Reg. UE n. 2024/1689, del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce norme armonizzate sull'intelligenza artificiale.

[3] Commissione europea, parere motivato C (2024) 7814 all'Italia.

normativa, un vero e proprio «pluralismo disfunzionale» che ostacola l'obiettivo di un mercato digitale unico e armonizzato. Il contesto emergenziale che spesso accompagna l'adozione di tecnologie IA contribuisce ad aggravare tali criticità, alimentando rischi di discriminazione algoritmica e di opacità decisionale. In Italia, le debolezze nella cultura della legalità costituzionale e nella valutazione preventiva degli impatti sui diritti fondamentali sono state più volte evidenziate dal Garante per la protezione dei dati personali[4]. Una regolazione dell'intelligenza artificiale realmente efficace non può dunque ridursi alla sola conformità formale al diritto europeo, ma deve promuovere una visione di sicurezza inclusiva, trasparente e fondata su solide garanzie procedurali. Questo articolo analizza il ruolo crescente dell'IA nelle forze dell'ordine, con particolare attenzione al bilanciamento tra esigenze di sicurezza e tutela della *privacy*. L'obiettivo è offrire una panoramica delle trasformazioni operative indotte dall'IA, dai sistemi di polizia predittiva al riconoscimento facciale, e delle relative implicazioni per i diritti civili. La ricerca esamina inoltre i principali nodi giuridici connessi all'impiego dell'IA, soffermandosi sul Regolamento generale sulla protezione dei dati (GDPR; reg. UE N. 2016/679) e sul più ampio quadro normativo europeo, valutandone l'adeguatezza rispetto alle sfide poste dalle tecnologie emergenti. Particolare attenzione è dedicata all'impatto delle norme dell'Unione europea sugli ordinamenti nazionali e alla coerenza delle politiche di sicurezza digitale nei diversi Stati membri. Accanto all'analisi giuridica, vengono affrontate le questioni etiche che l'impiego dell'IA solleva, evidenziando come tali tecnologie pongano interrogativi cruciali in tema di trasparenza, equità e responsabilità. Come sottolineato in letteratura, l'intelligenza artificiale può ridefinire i confini dei diritti individuali[5], rendendo necessario un approccio normativo innovativo e consapevole. Infine, il contributo propone raccomandazioni per un modello di sicurezza sostenibile e democratico, capace di coniugare innovazione tecnologica e tutela delle libertà fondamentali. La prospettiva, sviluppata in via principale con riferimento alla sicurezza pubblica interna, sarà da ultimo estesa al dominio militare e delle missioni internazionali, dove gli stessi nodi della delega decisionale alla macchina, della responsabilità e della supervisione umana si ripropongono in forma ancora più acuta.

2. Il ruolo dell'intelligenza artificiale nelle forze dell'ordine. L'integrazione delle tecnologie di intelligenza artificiale (IA) nelle forze dell'ordine rappresenta una trasformazione di rilievo nelle modalità di gestione della sicurezza pubblica e di prevenzione del crimine. Sul piano regolatorio, tali applicazioni si inseriscono in un perimetro di sicurezza definito dalla direttiva UE N. 2022/2555 (NIS 2), recepita in Italia con il d.lgs. n. 138/2024. Essa richiede che le piattaforme digitali e gli algoritmi impiegati dalle forze dell'ordine rispettino requisiti stringenti di resilienza informatica, garantendo continuità operativa e integrità dei dati. La l.n. 90/2024 rafforza questi obblighi e attribuisce all'Agenzia per la Cybersicurezza Nazionale (ACN) un ruolo centrale di vigilanza[6]. Tali misure incidono direttamente sulle modalità di impiego dell'IA nelle funzioni di pubblica sicurezza. Le tecnologie intelligenti possono esprimere appieno il proprio potenziale operativo soltanto se inserite in sistemi adeguatamente protetti e resilienti[7]. La tutela cibernetica delineata dalla direttiva NIS 2 e dalle relative norme italiane costituisce quindi un prerequisito essenziale per

[4] Garante per la protezione dei dati personali, parere n. 164/2021.
[5] European Union Agency for Fundamental Rights, *Getting the future right – Artificial intelligence and fundamental rights*, Lussemburgo, 2020, 1-3.
[6] M. Biagini, G. Zunino, *Cybersecurity, intelligenza artificiale e Difesa: riflessioni sulle normative europee e nazionali per un nuovo modello di regolamentazione nell'era dell'innovazione tecnologica accelerata*, in *Rivista elettronica di Diritto, Economia, Management*, 1, 2025, 13.
[7] *Ibidem*, 11.

un utilizzo efficace e sicuro dell'intelligenza artificiale da parte delle forze dell'ordine. Un ambito di particolare interesse riguarda le applicazioni attuali dell'IA. Esse mostrano con chiarezza l'impatto trasformativo che tali tecnologie esercitano sulle operazioni di polizia. La tecnologia di riconoscimento facciale, ad esempio, viene utilizzata per identificare sospetti e analizzare grandi quantità di informazioni visive. Gli algoritmi predittivi, a loro volta, consentono di stimare la probabilità di attività criminali sulla base di dati storici e variabili socio-economiche. Questi strumenti promettono di migliorare i processi decisionali, ottimizzare l'allocazione delle risorse e incrementare la sicurezza pubblica. La loro implementazione solleva tuttavia questioni delicate, rendendo necessaria un'analisi approfondita del rapporto tra politiche di sicurezza e adozione delle tecnologie IA. Una delle critiche principali riguarda la possibilità che l'impiego di dati storici sulla criminalità contribuisca a perpetuare pregiudizi sistemici. In tali casi, specifiche comunità o individui potrebbero essere colpiti in modo sproporzionato[8]. Si pone pertanto un interrogativo decisivo: come possono le forze dell'ordine assicurare che le strategie basate sull'IA non consolidino bias preesistenti o non conducano a errori giudiziari? Il perfezionamento degli strumenti investigativi basati sull'IA rende questi rischi ancora più meritevoli di una valutazione attenta e di una supervisione rigorosa. Un ulteriore ambito critico è rappresentato dal riconoscimento facciale. Nonostante il progresso tecnologico degli ultimi anni, il suo impiego può avere effetti rilevanti sui diritti fondamentali. I sistemi di riconoscimento facciale si basano su dati biometrici particolarmente sensibili e sollevano questioni legate alla privacy, al consenso e all'appropriatezza del trattamento[9]. Ciò richiede un equilibrio attento tra l'uso delle tecnologie per la prevenzione dei reati e la tutela dei diritti individuali. Occorre inoltre considerare l'impatto degli strumenti di analisi dei dati sui processi decisionali. Questi strumenti forniscono informazioni in tempo reale, aumentando l'efficienza operativa. Un'eccessiva dipendenza dai dati rischia però di marginalizzare elementi fondamentali dell'attività di polizia, come il giudizio umano, l'esperienza professionale e il rapporto con la comunità. Risulta quindi necessario individuare modalità attraverso cui l'IA possa integrare il contributo umano senza sostituirlo, favorendo un approccio cooperativo che valorizzi sia i progressi tecnologici sia la fiducia dei cittadini. L'adozione delle tecnologie IA implica anche sfide normative e giuridiche complesse. La conformità al GDPR rappresenta un obbligo imprescindibile, soprattutto in relazione al potenziale uso improprio dei dati personali, inclusi quelli biometrici. L'evoluzione del quadro normativo impone alle agenzie di pubblica sicurezza di definire politiche solide di gestione dei dati e di garantire che l'impiego dell'IA non comprometta i diritti degli individui. L'utilizzo responsabile dell'intelligenza artificiale richiede inoltre percorsi continui di formazione e aggiornamento, soprattutto per quanto riguarda le implicazioni etiche e i requisiti di conformità. Un ulteriore elemento riguarda la percezione dell'opinione pubblica. Atteggiamenti, timori e aspettative influenzano la legittimazione delle pratiche basate sull'IA e, di conseguenza, la loro efficacia. È quindi essenziale che le forze dell'ordine instaurino un dialogo trasparente con le comunità, affrontando le preoccupazioni relative alla privacy e alla sorveglianza. La costruzione della fiducia del pubblico costituisce un fattore determinante per il successo delle strategie di sicurezza fondate sull'IA. Infine, l'adattamento delle forze dell'ordine a queste tecnologie deve considerare le differenze normative esistenti nei vari ordinamenti, soprattutto all'interno dell'Unione europea. Ogni Stato membro adotta disposizioni specifiche in materia di tecnologia e protezione dei dati che incidono sulle modalità di impiego delle applicazioni IA. Una comprensione approfondita di tali differenze risulta fondamentale per un uso

[8] *European Union Agency for Fundamental Rights, Getting the future right*, cit., *passim*.
[9] G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Napoli, 2021.

responsabile ed efficace delle tecnologie. L'equilibrio tra il miglioramento dell'efficienza operativa e la tutela dei diritti alla privacy rimane uno dei temi centrali di questo dibattito. Considerata la complessità delle questioni in gioco, i paragrafi successivi offriranno un'analisi più approfondita degli strumenti di polizia predittiva, del riconoscimento facciale e delle tecniche di analisi dei dati, insieme ai dilemmi etici che tali strumenti inevitabilmente sollevano.

3. Bilanciare la sicurezza nazionale italiana e i diritti alla privacy nell'era dell'intelligenza artificiale. Nell'attuale contesto digitale, caratterizzato da un'evoluzione tecnologica sempre più rapida, il bilanciamento tra sicurezza nazionale e diritti fondamentali alla privacy rappresenta una delle sfide più significative per le democrazie contemporanee. L'adozione crescente di tecnologie di intelligenza artificiale (IA) da parte delle forze dell'ordine, impiegate per finalità di sorveglianza, prevenzione dei reati e supporto operativo, intensifica la tensione tra l'efficienza delle attività di sicurezza pubblica e la tutela delle libertà civili. In questo quadro, l'intreccio normativo tra il GDPR, il nuovo Regolamento europeo sull'intelligenza artificiale (*AI Act*) e il Codice italiano in materia di protezione dei dati personali (d.lgs. n. 196/2003, come modificato dal d.lgs. n. 101/2018)[10] assume un ruolo centrale. Il GDPR rappresenta il principale riferimento europeo per la tutela dei dati personali e impone standard elevati in materia di trasparenza, minimizzazione dei dati e liceità del trattamento. Il suo ambito, tuttavia, non copre integralmente le specificità dei sistemi di IA, soprattutto quando non sia immediatamente coinvolto un dato personale. Per colmare tali lacune interviene l'*AI Act*, approvato nel 2024 e attualmente in fase di recepimento. Esso introduce una classificazione dei sistemi di IA basata sul rischio e stabilisce requisiti stringenti per quelli considerati ad alto rischio, tra cui i software di riconoscimento facciale in tempo reale e i sistemi di profilazione predittiva. A differenza del GDPR, orientato alla tutela diretta dei diritti individuali, l'*AI Act* disciplina l'intero ciclo di vita tecnico dei sistemi di IA, prevedendo obblighi in materia di trasparenza, documentazione e supervisione umana. Il Codice privacy italiano svolge un ruolo complementare e rilevante. Esso recepisce i principi del GDPR adattandoli al contesto nazionale e include disposizioni settoriali dedicate, tra cui quelle relative ai trattamenti effettuati dalle forze dell'ordine, al lavoro e ai dati sanitari. Il Garante per la protezione dei dati personali è incaricato di assicurare il corretto equilibrio tra interesse pubblico e tutela dei diritti, fornendo linee guida interpretative e intervenendo nei casi di trattamenti illeciti. A questo quadro si aggiunge la prospettiva della cybersicurezza introdotta dalla direttiva NIS 2. In base alla direttiva NIS 2, recepita nell'ordinamento italiano con il d.lgs. n. 138/2024 e integrata dalla l.n. 90/2024, le unità di polizia e le autorità che impiegano sistemi di intelligenza artificiale sono oggi tenute ad adottare un approccio strutturato alla gestione del rischio informatico. In particolare, l'utilizzo di algoritmi predittivi e di piattaforme di riconoscimento facciale richiede la predisposizione di una valutazione formale del rischio cibernetico, l'adozione di misure di sicurezza *by design* integrate con i principi di *privacy by design*, nonché l'implementazione di procedure di notifica degli incidenti significativi, comprensive di un preallarme entro ventiquattro ore e di una relazione completa entro settantadue ore. Tali obblighi rafforzano la dimensione infrastrutturale della tutela dei diritti fondamentali, evidenziando come la protezione dei dati personali e la resilienza dei sistemi digitali costituiscano elementi inscindibili di un modello di sicurezza pubblica conforme allo Stato di diritto. La protezione dei diritti individuali e la resilienza cibernetica dei sistemi rappresentano due dimensioni inscindibili: l'IA non può essere considerata affidabile senza un'infrastruttura tecnologica sicura, ma la sicurezza pubblica perde legittimità

[10] D. lgs. n. 196/2003, *Codice in materia di protezione dei dati personali*, in G.U. 29 luglio 2003, n. 174, S.O. n. 123.

democratica quando non sono garantiti la liceità e la proporzionalità dei trattamenti[11]. Nonostante tali progressi, l'applicazione congiunta delle normative europee e nazionali può generare ambiguità interpretative e disomogeneità tra gli Stati membri, soprattutto nel settore della sicurezza pubblica. In Italia, l'efficacia delle tutele previste dall'*AI Act* dipenderà dalla capacità del legislatore di armonizzare i principi europei con il proprio quadro giuridico interno, evitando sovrapposizioni e lacune normative. Le tecnologie di IA, se progettate o impiegate in modo inadeguato, possono amplificare *bias* e discriminazioni, determinando forme di sorveglianza selettiva o decisioni arbitrarie[12]. Ciò solleva questioni di proporzionalità e legittimità che possono entrare in tensione con i principi costituzionali e con gli obblighi internazionali in materia di diritti fondamentali. Diventa quindi essenziale garantire un design etico e giuridicamente responsabile dei sistemi di IA, fondato su trasparenza algoritmica, supervisione umana effettiva e solide forme di *accountability*. Una tutela effettiva dei diritti non può prescindere dal coinvolgimento dell'opinione pubblica. La fiducia collettiva è un elemento essenziale per la legittimazione democratica dell'uso dell'intelligenza artificiale nella sicurezza pubblica. Solo un dialogo aperto, informato e partecipato può assicurare che l'innovazione tecnologica contribuisca al rafforzamento, e non all'erosione, dei diritti fondamentali. In conclusione, il bilanciamento tra sicurezza e privacy richiede un approccio multilivello e integrato, fondato sulla complementarità tra *AI Act*, GDPR e Codice privacy e sostenuto dalla responsabilità istituzionale e dalla partecipazione civica. Si tratta dell'unico percorso capace di garantire un uso dell'IA conforme ai principi dello Stato di diritto e ai valori democratici.

3.1. Il rapporto tra* AI Act*, GDPR e Codice* privacy*: un confronto sistematico. Il quadro normativo europeo e nazionale che disciplina l'impiego dell'intelligenza artificiale da parte delle forze dell'ordine si articola attorno a tre pilastri principali: il GDPR, il nuovo Regolamento europeo sull'intelligenza artificiale (*AI Act*) e il Codice italiano in materia di protezione dei dati personali. Il GDPR rappresenta il fondamento della tutela dei dati personali nell'Unione europea, applicandosi a qualsiasi trattamento di dati riferibili a persone fisiche. Esso è costruito su un approccio basato su principi generali, quali liceità, minimizzazione, proporzionalità e trasparenza, e riconosce agli interessati un articolato sistema di diritti, tra cui l'accesso, la rettifica e la cancellazione dei dati. Nell'ambito delle attività delle forze dell'ordine, il GDPR limita in modo significativo il trattamento dei dati biometrici e sensibili, imponendo l'esistenza di una base giuridica chiara e di garanzie rafforzate. L'*AI Act*, approvato nel 2024, si colloca su un piano differente ma complementare. Esso non è incentrato sui dati personali in quanto tali, bensì sui sistemi di intelligenza artificiale lungo l'intero ciclo di vita tecnologico. Il regolamento introduce una classificazione dei sistemi basata sul rischio, distinguendo tra applicazioni vietate, ad alto rischio, a rischio limitato e a rischio minimo. In questo quadro, molte applicazioni utilizzate dalle forze dell'ordine, quali i sistemi di riconoscimento facciale in tempo reale e gli algoritmi di profilazione predittiva, rientrano nella categoria dei sistemi ad alto rischio e sono pertanto soggette a obblighi stringenti in materia di trasparenza, documentazione tecnica, tracciabilità e supervisione umana. Il Codice *privacy* italiano svolge una funzione di raccordo tra il diritto europeo e l'ordinamento interno. Esso recepisce i principi del GDPR adattandoli alle specificità nazionali e prevede discipline settoriali, tra cui quelle relative ai trattamenti effettuati dalle autorità pubbliche e dalle forze dell'ordine. Il ruolo del Garante per la

[11] M. Biagini, G. Zunino, *Cybersecurity, intelligenza artificiale e Difesa*, cit., 13-14.
[12] *High-Level Expert Group on Artificial Intelligence (HLEG)* della Commissione europea, *Ethics Guidelines for Trustworthy AI*, 2019, *passim*.

protezione dei dati personali risulta centrale nel garantire il corretto bilanciamento tra interesse pubblico alla sicurezza e tutela dei diritti fondamentali, attraverso poteri di indirizzo, controllo e sanzione. Considerati nel loro insieme, *AI Act*, GDPR e Codice privacy delineano un sistema multilivello nel quale la protezione dei diritti fondamentali e la sicurezza tecnologica si rafforzano reciprocamente. Il GDPR assicura la tutela dei dati personali, l'*AI Act* governa i rischi strutturali connessi ai sistemi di intelligenza artificiale e il *Codice privacy* garantisce l'adattamento di tali principi al contesto nazionale. L'effettività di questo assetto dipenderà dalla capacità delle istituzioni di evitare sovrapposizioni normative e di assicurare un'applicazione coerente e coordinata delle diverse fonti.

4. Il quadro giuridico europeo e le sue implicazioni. L'avvento delle tecnologie di intelligenza artificiale (IA) ha determinato cambiamenti profondi in numerosi settori, in particolare nelle attività delle forze dell'ordine. Governi e agenzie di sicurezza, in Europa e a livello globale, cercano di sfruttare queste innovazioni per migliorare la sicurezza pubblica e l'efficienza operativa. La rapida integrazione dell'IA si confronta però con i quadri giuridici esistenti, e in particolare con la struttura normativa europea imperniata sul GDPR. La comprensione delle disposizioni specifiche del GDPR è fondamentale per valutare il suo impatto su giustizia e sicurezza in Europa. Il regolamento stabilisce standard elevati in materia di protezione dei dati e di tutela della *privacy*, valorizzando principi quali la minimizzazione dei dati, la limitazione delle finalità e la liceità del trattamento. Per le forze dell'ordine ciò si traduce in un quadro rigoroso che disciplina le modalità di raccolta, analisi e conservazione dei dati quando si ricorre a strumenti di IA, come il riconoscimento facciale e l'analisi predittiva. Sul versante dell'innovazione, la direttiva NIS 2 dialoga con l'*AI Act*. Quest'ultimo prevede un regime graduato di obblighi tecnici (documentazione, trasparenza, supervisione umana) per i sistemi considerati «ad alto rischio», tra cui rientrano tipicamente quelli utilizzati da polizia, dogane e altre autorità di contrasto. L'art. 57 dell'*AI Act* introduce inoltre le cosiddette *regulatory sandbox*, ossia ambienti di prova vigilati dalle autorità nazionali competenti (in Italia, AgID e ACN) nei quali è possibile sperimentare algoritmi di IA prima del loro impiego operativo. Il modello sotteso è quello di una regolamentazione «anticipatoria»: la sperimentazione in condizioni controllate consente alle autorità di individuare uno *sweet spot* tra capacità di governo della tecnologia e conoscenza dei suoi impatti, contribuendo a superare il noto «dilemma di *Collingridge*». In prospettiva, il prossimo *Cyber Resilience Act* è destinato a completare questo mosaico, estendendo requisiti di sicurezza anche ai dispositivi connessi impiegati in scenari di pubblica sicurezza[13]. Le differenze nel modo in cui i singoli Stati membri dell'Unione interpretano e attuano il GDPR possono tuttavia generare incoerenze nella regolamentazione dell'IA a livello europeo. Sebbene il GDPR offra una cornice giuridica unitaria, gli Stati godono di un margine di discrezionalità nell'adozione di misure nazionali specifiche, soprattutto in materia di attività di contrasto. Ciò produce approcci differenti che incidono sulla cooperazione transfrontaliera e sull'efficacia complessiva delle misure di sicurezza. In questo contesto, i casi di studio di Italia e Francia rappresentano due esempi significativi, seppur caratterizzati da strategie differenti nell'integrazione dell'IA nella sicurezza pubblica. Quanto al modello italiano, l'Italia ha adottato un approccio improntato a cautela, ponendo l'accento sulla necessità di disciplinare in modo rigoroso l'impiego delle tecnologie di IA nelle forze dell'ordine. Due casi risultano particolarmente emblematici. Il primo è il progetto SARI Real Time, promosso dal Ministero dell'interno per il riconoscimento facciale automatizzato. Il Garante per la protezione dei dati personali, nel parere n. 164 del 16 aprile 2021, si è espresso negativamente sull'uso del sistema

[13] M. Biagini, G. Zunino, *Cybersecurity, intelligenza artificiale e Difesa*, cit., 11-12.

per finalità di sicurezza pubblica, qualificandolo come una forma di sorveglianza biometrica di massa incompatibile con il GDPR (artt. 5, 6 e 9), in assenza di una base giuridica adeguata, di una valutazione d'impatto e di garanzie effettive. Secondo il Garante, l'impiego generalizzato del riconoscimento facciale in ambito urbano viola il principio di proporzionalità e mette a rischio privacy, libertà di movimento e anonimato. Il secondo è il caso del Comune di Trento, sanzionato per l'utilizzo illecito di tecnologie biometriche nei progetti europei MARVEL e PROTECTOR. Nel provvedimento n. 616 del 14 dicembre 2023, il Garante ha rilevato la mancanza dei presupposti di liceità, l'assenza di garanzie adeguate e di valutazioni d'impatto, disponendo la cancellazione dei dati trattati e irrogando una sanzione di 50.000 euro. Il caso mette in luce il rischio che la ricerca pubblica e i progetti sperimentali diventino ambiti di «sospensione» normativa, nei quali i diritti fondamentali risultano di fatto subordinati alle esigenze di innovazione. Nel complesso, l'Autorità italiana per la protezione dei dati personali ha più volte sottolineato l'esigenza di bilanciare innovazione e tutela dei diritti fondamentali, promuovendo valutazioni rigorose dei sistemi di IA prima della loro implementazione; ne deriva un quadro che tende a privilegiare trasparenza, responsabilità e controllo pubblico, in coerenza con i principi del GDPR. La Francia ha adottato invece un'impostazione più proiettata verso la sperimentazione e l'uso delle tecnologie di IA nella sicurezza pubblica. Il governo francese ha promosso diversi programmi pilota, in particolare nell'ambito della sicurezza urbana, con l'obiettivo dichiarato di rafforzare le capacità di prevenzione e gestione dei reati: vi rientrano, ad esempio, sistemi di videosorveglianza «intelligente» e strumenti di analisi predittiva applicati a grandi centri urbani ed eventi di massa. Questo approccio, più permissivo sul piano sperimentale, ha suscitato critiche da parte di associazioni per i diritti civili e difensori della privacy, preoccupati per il rischio di sorveglianza pervasiva e di limitazioni indirette delle libertà fondamentali. Il dibattito si concentra in particolare sull'adeguatezza delle garanzie previste dal GDPR rispetto all'uso intensivo di tecnologie biometrico-predittive in contesti di polizia amministrativa e giudiziaria. Le differenze tra il modello italiano, più prudente e orientato alla centralità delle garanzie, e quello francese, maggiormente sperimentale, mostrano come le interpretazioni nazionali del GDPR possano condurre a implementazioni molto diverse dell'IA nelle forze dell'ordine. Ciò incide non solo sulla cooperazione tra autorità di polizia dei vari Paesi, ma anche sulla percezione di omogeneità delle tutele riconosciute ai cittadini nello spazio giuridico europeo. L'esperienza comparata suggerisce che il problema principale non risiede nella maggiore o minore apertura alla sperimentazione tecnologica, bensì nella capacità delle istituzioni di garantire trasparenza, controllo democratico e responsabilità effettiva nell'impiego dei sistemi di intelligenza artificiale. In questa prospettiva, l'innovazione tecnologica non può essere considerata un valore autonomo, ma deve essere costantemente misurata alla luce della tutela dei diritti fondamentali e dei principi dello Stato di diritto.

5. L'intelligenza artificiale nei contesti operativi internazionali. Le criticità sin qui esaminate con riferimento alla sicurezza pubblica interna non restano confinate a tale ambito: esse si ripropongono, in forma ancora più acuta, nei contesti militari e nelle missioni operative internazionali, dove la delega decisionale alla macchina, l'opacità algoritmica e la frammentazione della responsabilità incidono direttamente sulla vita e sull'incolumità delle persone. Lo stesso interrogativo che attraversa l'impiego dell'IA nelle forze dell'ordine, ossia come preservare un controllo umano effettivo e una catena di responsabilità a fronte di sistemi sempre più autonomi, si pone dunque, con intensità maggiore, sul terreno della difesa. In questo senso, il settore della sicurezza pubblica può essere considerato un laboratorio normativo e operativo per comprendere le problematiche che emergono nei contesti militari, nei quali le conseguenze di eventuali errori algoritmici risultano potenzialmente più gravi e

difficilmente reversibili. L'utilizzo crescente dell'intelligenza artificiale (IA) nei contesti militari e nelle missioni operative internazionali solleva infatti questioni tecniche, etico-giuridiche e geopolitiche di grande rilevanza. Tali scenari includono operazioni condotte sotto l'egida delle Nazioni Unite, della NATO o in coalizioni *ad hoc*, nelle quali la cooperazione tra Stati e l'impiego di tecnologie avanzate rendono più complessa l'applicazione del diritto internazionale. L'IA è impiegata oggi in una vasta gamma di funzioni: dall'analisi dei dati di intelligence alla sorveglianza automatizzata tramite droni, dall'identificazione autonoma dei bersagli alla pianificazione strategica assistita. Questi sistemi promettono maggiore efficienza operativa e una riduzione dei rischi per il personale militare, pur introducendo il pericolo di una delega decisionale ad entità non umane, soprattutto nei casi in cui si riduce o si elimina il controllo umano diretto. Nel settore della Difesa, l'IA deve poggiare su un'infrastruttura di tipo *zero trust*, in grado di resistere ad attacchi diretti alle reti di comando e controllo (C2), ai sensori ISR e ai *data lake* di intelligence. Il d.lgs. n. 138/2024, che recepisce la direttiva NIS 2 estendendola al perimetro di sicurezza nazionale cibernetica, introduce per le forze armate obblighi di rafforzamento progressivo delle infrastrutture, tra cui l'inventario dei sistemi critici, l'analisi del rischio cyber, i piani di continuità operativa e l'esecuzione periodica di esercitazioni di risposta agli incidenti (*cyber drills*). Come evidenziato da Biagini e Zunino, in assenza di misure adeguate un modello decisionale potenziato dall'IA può trasformarsi nel *single point of failure* di un'intera operazione militare; ne deriva la necessità di coordinare il comando operazioni in rete con le *cyber-unit* della NATO e di integrare gli standard STANAG per la condivisione sicura dei dati tattici[14]. Un esempio particolarmente emblematico è rappresentato dai sistemi d'arma letali autonomi (LAWS), capaci di selezionare e attaccare obiettivi senza intervento umano. Sebbene ad oggi non esista un divieto giuridico internazionale espresso, diverse organizzazioni, tra cui il Comitato internazionale della Croce Rossa, hanno richiesto una moratoria o una regolamentazione vincolante in linea con i principi del diritto internazionale umanitario[15]. L'introduzione dell'IA comporta inoltre trasformazioni profonde nelle regole d'ingaggio (*Rules of Engagement*, RoE), che possono essere influenzate da algoritmi in grado di suggerire l'uso della forza sulla base di analisi predittive comportamentali. Questa automatizzazione rischia di compromettere il rispetto dei principi di distinzione e proporzionalità, cardini fondamentali del diritto dei conflitti armati[16]. Le sfide diventano ancora più complesse se si considerano le implicazioni per il diritto internazionale umanitario e per la tutela dei diritti umani. Sistemi semi-autonomi possono non essere in grado di distinguere con sufficiente affidabilità tra civili e combattenti, né di adattarsi alle situazioni mutevoli e spesso caotiche che caratterizzano i teatri di guerra. Ciò espone a potenziali violazioni delle Convenzioni di Ginevra, in particolare in materia di protezione dei civili, necessità militare e trattamento delle persone fuori combattimento[17]. Le questioni legate alla responsabilità legale assumono una rilevanza ancora maggiore nei contesti internazionali. L'opacità degli algoritmi e la frammentazione decisionale tra Stati rendono difficile attribuire la responsabilità in caso di errore. Sorgono interrogativi complessi: chi risponde se un drone armato guidato da IA colpisce civili? Il comandante sul campo, il programmatore del software, lo Stato che ha sviluppato la tecnologia, o quello che la impiega? Questi dilemmi risultano esemplificati dal caso dell'Afghanistan, dove i droni *AeroVironment Switchblade,* impiegati dal 2012 per attacchi mirati e attività di raccolta dati in combinazione con sistemi di IA, hanno sollevato dubbi

[14] *Ibidem*, 15-17.
[15] Comitato Internazionale della Croce Rossa, *Ethics and Autonomous Weapon Systems*, 2021.
[16] P. Asaro, *On Banning Autonomous Weapon Systems: Human Rights, Automation, and the Dehumanization of Lethal Decision-Making*, in *International Review of the Red Cross*, 2012.
[17] Convenzioni di Ginevra e Protocolli aggiuntivi I e II, 1977.

giuridici ed etici significativi, soprattutto in relazione alla responsabilità per le vittime civili[18]. Di fronte a tali problematiche, una parte crescente della dottrina propone l'adozione di un principio di responsabilità condivisa tra Stati utilizzatori e produttori delle tecnologie, unito a obblighi di trasparenza, tracciabilità e supervisione umana continua. Secondo questa prospettiva, solo una responsabilità multilivello può fornire un quadro adeguato alla complessità delle operazioni militari contemporanee che integrano sistemi di IA. Si conferma così, sul terreno della difesa, lo stesso nodo emerso nel contesto della sicurezza pubblica: l'efficacia operativa dell'IA resta legittima solo finché è accompagnata da un'effettiva imputazione della responsabilità. Ne deriva che le garanzie di trasparenza, supervisione umana e accountability non costituiscono limiti esterni all'innovazione tecnologica, bensì condizioni essenziali per la sua compatibilità con i principi dello Stato di diritto e con il diritto internazionale umanitario.

6. Considerazioni etiche nell'impiego dell'IA. La rapida integrazione delle tecnologie di intelligenza artificiale (IA) nelle forze dell'ordine solleva questioni etiche di notevole complessità, che richiedono un'analisi approfondita. L'impiego dell'IA in questo settore offre opportunità significative per migliorare l'efficienza operativa, la capacità predittiva e la prevenzione del crimine. Tuttavia, tali vantaggi devono essere ponderati attentamente alla luce delle preoccupazioni etiche connesse alla responsabilità, alla parzialità algoritmica e alla possibile violazione delle libertà civili. Un primo interrogativo riguarda gli standard etici che dovrebbero governare l'adozione delle tecnologie di IA da parte delle forze dell'ordine. L'introduzione di sistemi intelligenti richiede linee guida capaci di tutelare in modo effettivo i diritti umani e i valori fondamentali delle società democratiche. Questi standard devono guidare sia lo sviluppo sia l'utilizzo operativo degli strumenti di IA, prevenendo forme di sorveglianza sproporzionata, discriminazioni sistemiche o decisioni automatizzate prive di adeguate garanzie. Principi come trasparenza, equità, rispetto della privacy e responsabilità devono essere definiti con chiarezza e integrati nelle pratiche operative: in quest'ottica, la trasparenza implica che gli algoritmi siano comprensibili e verificabili, mentre l'equità richiede un controllo intenso dei dataset e una costante verifica dell'assenza di *bias* in grado di colpire in modo sproporzionato le comunità vulnerabili. Il problema della parzialità algoritmica rappresenta una delle sfide più rilevanti. Molti sistemi di IA, come quelli utilizzati nella polizia predittiva o nel riconoscimento facciale, sono addestrati su dati che riflettono pregiudizi storici o squilibri socioeconomici. Questo può condurre a decisioni discriminatorie, potenzialmente aggravando le disuguaglianze già presenti nel tessuto sociale. Per mitigare tali rischi, è essenziale che le forze dell'ordine adottino strategie mirate: utilizzo di dataset diversificati e controllati, audit periodici dei sistemi, coinvolgimento della comunità attraverso processi partecipativi che consentano di raccogliere osservazioni e valutazioni sull'impatto delle tecnologie. Il coinvolgimento della cittadinanza, inoltre, contribuisce a rafforzare la legittimità dell'uso dell'IA e a consolidare il rapporto di fiducia tra istituzioni e popolazione. Un'ulteriore questione etica riguarda la responsabilità. È indispensabile stabilire meccanismi chiari che consentano di attribuire la responsabilità delle decisioni algoritmiche. Cosa accade, ad esempio, se un sistema di IA formula una previsione errata che conduce a un arresto ingiustificato? Per rispondere a questa domanda occorre definire un modello di responsabilità che coinvolga sviluppatori, decisori politici e operatori delle forze dell'ordine. A tal fine, la documentazione dettagliata dei processi di progettazione dell'IA e dei flussi decisionali rappresenta una buona pratica imprescindibile. L'istituzione di comitati di supervisione dotati di una partecipazione della società civile può inoltre garantire un controllo

[18]M. Zenko, *Reforming U.S. Drone Strike Policies*, *Council on Foreign Relations*, 2013.

più rigoroso e contribuire a mantenere l'utilizzo delle tecnologie entro i limiti delle norme etiche e sociali condivise. La fiducia del pubblico nelle istituzioni di sicurezza è profondamente influenzata dalle modalità con cui l'IA viene implementata. La percezione di strumenti tecnologici invasivi o ingiusti può intensificare il distacco tra comunità e forze dell'ordine, minando l'efficacia stessa delle politiche di sicurezza. Per questo motivo, l'impegno pubblico e la comunicazione trasparente rappresentano elementi fondamentali: spiegare come funziona l'IA, quali garanzie offre e quali limiti operativi sono stati stabiliti contribuisce a creare un senso di partecipazione e una corresponsabilità collettiva. L'introduzione dell'IA nelle attività di polizia apre inevitabilmente una discussione sul rapporto tra tecnologia e diritti umani. Le capacità predittive e di analisi avanzata dei sistemi intelligenti incidono direttamente su diritti fondamentali quali la privacy, la non discriminazione e il diritto a un giusto processo. Le forze dell'ordine, in quanto istituzioni con un mandato pubblico, hanno l'obbligo di garantire che tali diritti non vengano compromessi. Su questo punto, Biagini e Zunino sottolineano che la sfida etica non riguarda solo ciò che fa l'IA, ma soprattutto chi risponde delle sue conseguenze: di qui la proposta di un approccio orientato alla *accountability-by-design*, fondato sull'integrazione strutturale di trasparenza, sicurezza e responsabilità sin dalle prime fasi di sviluppo dei sistemi di intelligenza artificiale. Tale modello si articola, in primo luogo, nell'adozione di algoritmi *explainable*, capaci di produrre tracce verificabili del processo decisionale; in secondo luogo, nella previsione di registri obbligatori delle attività, come richiesto dall'*AI Act* per i sistemi ad alto rischio, funzionali alle analisi forensi e al controllo pubblico; infine, nell'esecuzione di audit periodici di sicurezza, coerenti con i requisiti infrastrutturali introdotti dalla direttiva NIS 2. Attraverso questi strumenti, la catena di comando conserva sempre un anello umano di responsabilità giuridica, evitando che decisioni automatizzate e opache producano forme di deresponsabilizzazione istituzionale o, come è stato efficacemente osservato in dottrina, una vera e propria «autonomizzazione dell'errore». L'integrazione di *explainability*, *log* verificabili e audit di sicurezza permette di concretizzare i principi di trasparenza, equità e fiducia richiamati in precedenza, rafforzando il legame tra tutela dei diritti umani e legittimità dell'azione di polizia supportata dall'IA[19].

7. Conclusione. L'integrazione dell'intelligenza artificiale nelle forze dell'ordine si presenta come una sfida complessa, nella quale il progresso tecnologico si confronta direttamente con la necessità di tutelare i diritti fondamentali. Le analisi condotte hanno mostrato come gli strumenti basati su IA possano offrire benefici rilevanti in termini di efficienza operativa e capacità predittiva; tuttavia, tali vantaggi si accompagnano a interrogativi significativi in tema di protezione della *privacy*, trasparenza delle decisioni automatizzate e garanzie delle libertà civili. È emerso con evidenza che gli attuali quadri normativi non risultano pienamente adeguati a governare l'impatto delle tecnologie intelligenti. Molte disposizioni sono state elaborate in un contesto tecnologico ormai superato e richiedono un aggiornamento che consenta di affrontare le sfide della contemporaneità. Per questo il legislatore è chiamato a definire standard giuridici solidi e coerenti, capaci di orientare l'impiego dell'IA senza compromettere i valori dello Stato di diritto. Parallelamente, si rende necessario un approccio collaborativo e multidisciplinare alla governance dell'intelligenza artificiale. Lo sviluppo di politiche efficaci richiede il coinvolgimento di sviluppatori, istituzioni pubbliche, forze dell'ordine, esperti di etica e organizzazioni della società civile. Solo un dialogo costante tra tali attori può favorire un equilibrio sostenibile tra esigenze di sicurezza e tutela dei diritti. In questo quadro, la definizione di meccanismi di governance etica fondati su responsabilità,

[19] M. Biagini, G. Zunino, *Cybersecurity, intelligenza artificiale e Difesa*, cit., 18-19.

trasparenza e supervisione umana rappresenta un requisito essenziale per un utilizzo legittimo dell'IA. Un ruolo altrettanto decisivo è svolto dall'opinione pubblica. La fiducia dei cittadini nelle istituzioni che adottano tecnologie avanzate dipende in larga misura dalla percezione di equità, legittimità e protezione dei diritti. Promuovere un dialogo aperto e partecipato con le comunità può contribuire a rafforzare il consenso sociale e a migliorare l'efficacia degli interventi di sicurezza pubblica. Sul piano internazionale, l'Europa è chiamata a estendere la propria visione regolatoria oltre i confini dell'Unione, includendo nel confronto globale anche i Paesi che rischiano di rimanere esclusi dal progresso tecnologico, come quelli del continente africano. La cooperazione internazionale e lo scambio di buone pratiche possono favorire un modello di sviluppo inclusivo, equo e rispettoso dei diritti umani. In definitiva, la costruzione di un sistema di regolazione efficace e responsabile dell'intelligenza artificiale nelle forze dell'ordine richiede non solo un aggiornamento delle norme e delle prassi istituzionali, ma anche un profondo cambiamento culturale. Solo un impegno costante verso la tutela dei diritti, l'etica pubblica e la cooperazione internazionale potrà garantire che la tecnologia contribuisca realmente alla sicurezza collettiva senza erodere i principi fondamentali della democrazia.

Abstract. Il presente contributo analizza l'impiego crescente dell'intelligenza artificiale nei settori della sicurezza e della difesa, incluso l'ambito militare, con particolare attenzione al bilanciamento tra esigenze di ordine pubblico e sicurezza nazionale, da un lato, e tutela dei diritti fondamentali, *in primis* la *privacy*, dall'altro. Le tecnologie di sorveglianza intelligente, gli algoritmi predittivi e i sistemi decisionali automatizzati stanno trasformando l'operatività delle forze dell'ordine, riducendo progressivamente il controllo umano. Questa transizione solleva importanti questioni etiche, giuridiche e politiche. Lo studio esamina in particolare il contesto italiano, soffermandosi sul disegno di legge sull'intelligenza artificiale, giudicato dalla Commissione europea (parere C(2024) 7814) non pienamente conforme all'*AI Act*. L'analisi mette in luce le tensioni tra l'esigenza di sicurezza e la protezione della privacy, sottolineando le lacune strutturali nella governance dell'IA e nei meccanismi di supervisione democratica. In prospettiva comparata, lo studio considera le esperienze di altri Stati membri dell'Unione europea, valutando l'efficacia degli strumenti regolatori e la coerenza con i principi costituzionali e convenzionali in materia di diritti umani.

Abstract. This contribution examines the growing use of artificial intelligence in the fields of security and defence, including the military domain, with particular attention to the balance between public order and national security needs, on the one hand, and the protection of fundamental rights, primarily privacy, on the other. Intelligent surveillance technologies, predictive algorithms and automated decision-making systems are progressively transforming law enforcement operations, leading to a gradual reduction of human oversight. This development raises significant ethical, legal and political concerns. The study focuses in particular on the Italian context, analysing the draft law on artificial intelligence, which has been considered by the European Commission, in its Opinion C(2024) 7814, not fully compliant with the AI Act. The analysis highlights the tensions between security requirements and the protection of privacy, emphasising structural shortcomings in artificial intelligence governance and in mechanisms of democratic oversight. From a comparative perspective, the study also considers the experiences of other Member States of the European Union, assessing the effectiveness of regulatory instruments and their consistency with constitutional and conventional principles concerning the protection of human rights.

Parole chiave. Intelligenza artificiale – Sicurezza – Privacy – *AI Act* – Forze dell'ordine – Diritto europeo.

Key words. Artificial Intelligence – Security – Privacy – AI Act – Law Enforcement – European Law.