Il ricorso all'intelligenza artificiale nel contesto di attività di *law enforcement* e di operazioni militari: brevi riflessioni nella prospettiva del diritto internazionale

di Elena Carpanelli

Abstract: *Artificial Intelligence in the Field of Law Enforcement and in Military Operations: An International Law Perspective* – The present paper analyses the use of predictive algorithms in law enforcement and military settings from the perspective of international human rights law and international humanitarian law. In doing so, it relies on a two-fold approach: on the one hand, it highlights the possible incompatibilities of the use of such technology with international norms; on the other hand, it stresses the importance of taking into account these same norms for the purpose of identifying a common accountability framework for the use of AI systems, including predictive algorithms.

Keywords: Predictive policing; Artificial intelligence; Military operations; International Law; Human Rights.

1. Introduzione

Negli ultimi anni, si è assistito a un ricorso crescente, da parte delle forze dell'ordine, ad algoritmi che, attraverso l'incrocio di un'elevata quantità di dati provenienti da fonti diverse, permettono di prevedere, tra l'altro, la pericolosità sociale di un individuo, la commissione di un reato ovvero la sua localizzazione[1]. In Canada, ad esempio, sia il Dipartimento di polizia di Vancouver sia il Saskatoon Police Service hanno confermato di utilizzare, o di essere in procinto di utilizzare, algoritmi al fine di prevenire il compimento di reati[2]. Negli Stati Uniti, da oltre un decennio le forze dell'ordine di numerose città fanno ricorso a software elaborati, spesso gestiti da società private, come Geolitica (ex PredPol) o Shotspotter, per fini di polizia predittiva[3]. Tecniche di polizia predittiva sono utilizzate anche in Europa. In Italia, ad esempio, le forze di polizia si avvalgono del sistema

[1] Si rinvia, tra gli altri, a I. Mugari, E. E. Obioha, *Predictive Policing in the United States of America and in Europe: Trends in a Decade of Research and the Future of Predictive Policing*, in *Social Science*, 10, 2021, 234 ss.

[2] Si rimanda al rapporto di TheCitizenLab, *To Surveil and Predict. A Human Rights Analysis of Algorithmic Policing in Canada*, 2020, 2.

[3] I dati aggiornati sono disponibili al sito: atlasofsurveillance.org/search?utf8=%E2%9C%93&location=&technologies%5B86%5D=on.

DPCE online
ISSN: 2037-6677

Dynamic Evolving Learning Integrated Alghoritm (Delia) (ex KeyCrime), che analizza le condotte delittuose per prevedere il compimento di reati in specifiche aree ed elaborare profili criminali[4].

L'utilizzo di algoritmi nello svolgimento di funzioni di protezione della sicurezza pubblica consentirebbe non solo di ridurre il crimine, ma anche di garantire una distribuzione più efficiente delle risorse umane disponibili. Tuttavia, simili tecniche predittive possono altresì interferire con il godimento di alcuni diritti fondamentali[5]. Come è stato osservato, infatti, il ricorso a tali algoritmi può enfatizzare le discriminazioni già esistenti e avere effetti negativi sulla tutela dei diritti alla privacy, alla protezione dei dati, e alla libertà di espressione[6].

Proprio alla luce di alcune di queste considerazioni, nel mese di giugno 2020, la città di Santa Cruz, in California, ha vietato il ricorso ad algoritmi per fini di polizia predittiva[7], seguita da altre città statunitensi[8]. Inoltre, il 6 ottobre 2021, il Parlamento europeo ha espresso la propria opposizione rispetto all'utilizzo dell'intelligenza artificiale, da parte delle autorità di polizia, per fare previsioni sui comportamenti individuali o di gruppo sulla base di dati storici o condotte precedenti, dell'appartenenza a un gruppo, dell'ubicazione o di altre caratteristiche[9]. Ciò in ragione sia della scarsa accuratezza di tali previsioni sia delle loro implicazioni discriminatorie[10].

Tuttavia, tali tecniche continuano a essere largamente utilizzate. Inoltre, il ricorso ad algoritmi predittivi ha iniziato a essere prospettato anche rispetto a operazioni militari, allo scopo, tra l'altro, di individuare i possibili nemici e prevederne le mosse, con evidenti ripercussioni in termini di detenzione e *targeting*[11]. Ad esempio, nel mese di luglio 2021, il North American Aerospace Defence Command e il United States Northern Command hanno svolto la terza serie di test su alcune tecnologie basate sull'intelligenza artificiale, che dovrebbero rendere più efficiente e veloce il processo decisionale da parte dei comandanti militari[12].

Il presente breve contributo intende analizzare il ricorso ad algoritmi

[4] Si rinvia al rapporto dell'organizzazione non governativa FairTrials, *Automating Injustice: The Use of Artificial Intelligence & Automatic Decision-Making Systems in Criminal Justice in Europe*, 9 settembre 2021, 20.
[5] Sul tema si rinvia, tra l'altro, ad Agenzia dei diritti fondamentali dell'Unione europea, *Artificial Intelligence and Fundamental Rights*, dicembre 2020, 34.
[6] Si rimanda, tra gli altri, a A. Bonfanti, *Big Data e polizia predittiva: riflessioni in tema di protezione del diritto alla privacy e dei dati personali*, in *MediaLaws - Rivista del diritto dei media*, 3, 2018, 1-13.
[7] See A. Asher-Schapiro, *California City Bans Bans Predicting Policing in U.S. First*, in *Reuters*, 24 giugno 2020.
[8] Tra cui New York e Cambridge. Si rimanda a Parlamento europeo, Risoluzione sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale, 6 ottobre 2021, par. 24.
[9] Ibid.
[10] Ibid.
[11] A. S. Deeks, *Predicting Enemies*, in *Virginia Law Review*, 8, 2018, 1529-1592.
[12] N. Bajema, *Pentagon Wants AI to Predict Events Before they Occur*, in *IEEE Spectrum*, 14 ottobre 2021.

predittivi nella prospettiva della tutela dei diritti umani e del diritto umanitario al fine di contribuire al dibattito concernente i possibili sviluppi in termini di regolamentazione futura. A tal fine, dopo avere esaminato l'impatto dell'utilizzo dell'intelligenza artificiale a fini di polizia predittiva sulla tutela dei diritti umani (par. 2.1), lo studio si focalizzerà sull'importanza di un approccio "human rights-based" ai fini della regolamentazione della materia, svolgendo alcune riflessioni, del tutto preliminari, sulla recente proposta di regolamento sull'intelligenza artificiale dell'Unione europea (par. 2.2.). L'analisi si rivolgerà, quindi, ai possibili profili di incompatibilità dell'utilizzo di algoritmi predittivi durante la conduzione di operazioni militari con la tutela dei diritti umani e il diritto umanitario, nonché sull'esigenza di una regolamentazione chiara ed efficace in materia (par. 3).

2. L'utilizzo dell'intelligenza artificiale per fini di polizia predittiva

2.1. Ricorso ad algoritmi per fini di polizia predittiva e tutela dei diritti umani

Come è stato sottolineato in uno studio su algoritmi e diritti umani realizzato dal Consiglio d'Europa, «the wide of sectors in which automated decision-making systems are employed can have serious repercussions on human rights»[13]. Tali settori includono l'esercizio di funzioni di prevenzione e repressione del crimine e protezione della pubblica sicurezza[14]. L'utilizzo dell'intelligenza artificiale per fini di polizia predittiva può infatti incidere sul godimento di molteplici diritti umani, tutelati sia a livello nazionale sia sul piano internazionale.

Innanzitutto, come sottolineato anche dal Comitato delle Nazioni Unite per l'eliminazione di ogni forma di discriminazione razziale, il ricorso a tecniche predittive nel settore della sicurezza ha il potenziale di acuire il razzismo, la discriminazione razziale, la xenofobia e altre forme di esclusione[15]. Il ricorso ad algoritmi predittivi, che si fonda su un'attività di profilazione, comporta, infatti, il rischio di un aumentato pregiudizio nei confronti di alcuni individui o gruppi di individui e può determinare condotte discriminatorie, anche, ancorché non esclusivamente, su base razziale. Ciò in violazione del divieto di discriminazione e del principio di eguaglianza dinanzi alla legge, sanciti, tra l'altro, dalla stessa Convenzione delle Nazioni Unite per l'eliminazione di ogni forma di discriminazione razziale[16]. Come

[13] Studio del Consiglio d'Europa, *Algorithms and Human Rights*, DGI(2017)12, marzo 2018, 24.
[14] Ibid.
[15] Raccomandazione generale n. 36(2020) on preventing and combating racial profiling by law enforcement officials, 17 dicembre 2020, doc. CERD/C/GC/36, par. 12.
[16] New York, 7 marzo 1966, entrata in vigore il 4 gennaio 1969, 660 UNTS 195, articoli 2 e 5. Sulla incompatibilità di forme di profilazione razziale con il divieto di discriminazione si rimanda, tra gli altri, anche a Comitato dei diritti umani, Constatazioni, Williams Lecraft c. Spagna, doc. CCPR/C/96/D/1495/2006, 27 luglio 2009.

DPCE online
ISSN: 2037-6677

osservato dallo stesso Comitato, ad esempio, «historical arrest data about a neighbourhood may reflect racially biased policing practices. If fed into a predictive policing model, use of these data poses a risk of steering future predictions in the same, biased direction, leading to overpolicing of the same neighbourhood, which in turn may lead to more arrests in that neighbourhood, creating a dangerous feedback loop»[17].

Inoltre, le tecniche predittive utilizzate dalle forze dell'ordine, fondandosi sulla raccolta pervasiva, il trattamento automatizzato e l'incrocio di grandi quantità di dati, pongono problemi di incompatibilità anche con la tutela dei diritti alla privacy e alla protezione dei dati[18]. Peraltro, se è vero che tali diritti possono essere limitati per ragioni di pubblica sicurezza, simili restrizioni devono essere previste dalla legge e costituire una misura necessaria in una società democratica[19]. È tuttavia dubbio se la raccolta generalizzata e il trattamento di dati alla base del processo predittivo possano ritenersi necessari in una società democratica. Seppur in casi non concernenti sistemi di polizia predittiva, la Corte europea dei diritti umani e la Corte di giustizia dell'Unione europea hanno ritenuto, infatti, che la raccolta pervasiva di dati e il loro trattamento da parte di autorità di pubblica sicurezza, in assenza di adeguate garanzie contro possibili abusi, fosse incompatibile con la tutela dei diritti alla privacy e alla protezione dei dati[20].

Qualora implichino una sorveglianza delle comunicazioni online o il riconoscimento facciale dei partecipanti a una manifestazione, i sistemi di polizia predittiva possono altresì interferire nel godimento del diritto alla libertà d'espressione e di riunione pacifica, tutelati, tra l'altro dal Patto internazionale sui diritti civili e politici[21] e dalla Convenzione europea dei diritti umani[22]. Infatti, «the use of algorithmic social media mining tools to monitor online conversations about or among targeted subjects increases the risk that individuals will engage in self-censorship if they know or suspect that their speech is being monitored by government agencies. Similarly, individuals may avoid freely exercising their freedom of

[17] Ibid., p. 33.
[18] Per un'analisi più dettagliata si rimanda nuovamente a A. Bonfanti, *Big Data e polizia predittiva: riflessioni in tema di protezione del diritto alla privacy e dei dati personali*, cit., 1-13.
[19] Si rinvia, ad esempio, all'art. 8 della Convenzione per la salvaguardia dei diritti umani e delle libertà fondamentali (o Convenzione europea dei diritti umani) (Roma, 4 novembre 1950).
[20] In senso contrario, si vedano, ad esempio, Corte europea dei diritti umani, Grande Camera, *Roman Zakharov c. Russia*, ricorso n. 47143/06, sentenza del 4 dicembre 2015. Si veda anche Corte europea dei diritti umani, Grande Camera, *Big Brother Watch e altri c. Regno Unito*, ricorsi n. 58170/13, 62322/14, 24969/15, sentenza del 25 maggio 2021. In modo analogo, si veda Corte di giustizia dell'Unione europea, *Digital Rights Ireland.* cause riunite C-293/12 e C-594/12, sentenza dell'8 aprile 2014. La Corte, in questo caso, ha dichiarato invalida la direttiva 2006/24/CE sulla base degli artt. 7, 8 e 52 della Carta dei diritti fondamentali dell'Unione europea.
[21] Articoli 19 e 21.
[22] Articoli 10 e 11.

association if police algorithms are used to track social networks and group affiliations, such as through (…) algorithmic social network analysis system, or even if individuals only suspect that the police may be tracking such information»[23]. Anche tali diritti possono subire limitazioni per ragioni di pubblica sicurezza. Tuttavia, anche in questo caso è dubbio se, in mancanza di parametri chiari che circoscrivano la sorveglianza e di garanzie contro possibili abusi, simili restrizioni nel godimento dei diritti poc'anzi menzionati possano ritenersi necessarie in una società democratica.

Laddove rendano più probabile l'arresto di determinati individui, le tecniche predittive per fini di polizia rischiano, inoltre, di incidere sul godimento del diritto alla libertà personale, che implica il divieto di detenzione arbitraria[24].

A ciò si aggiunga che l'assenza di trasparenza e accessibilità, che può caratterizzare il processo decisionale legato al ricorso ad algoritmi per fini di polizia predittiva, solleva problemi di compatibilità anche con alcune garanzie procedurali, tra cui l'esercizio del diritto di difesa[25].

Infine, nel caso in cui la previsione del compimento di un reato si traduca nell'uso arbitrario della forza letale, magari ad opera di sistemi autonomi, le tecniche predittive potrebbero avere un impatto negativo sull'esercizio del diritto alla vita[26].

Tanto premesso, come è stato suggerito, analizzare il ricorso ad algoritmi nella prospettiva della tutela dei diritti umani permette non solo di stabilire se un determinato utilizzo violi o meno le norme esistenti, ma anche di sviluppare un "accountability framework" in materia[27]. Infatti, le norme internazionali concernenti la tutela dei diritti umani pongono in capo agli Stati non solo obblighi negativi ma anche obblighi positivi, in termini di prevenzione e repressione delle violazioni, anche rispetto a condotte di privati. Conseguentemente, esse sarebbero in grado di «bring clarity regarding the actions that States and businesses are expected to take and the consequences of failing to act»[28]. In tale prospettiva, un approccio fondato

[23] Si rimanda nuovamente a TheCitizenLab, *To Surveil and Predict. A Human Rights Analysis of Algorithmic Policing in Canada*, cit., 97.
[24] Tale diritto è tutelato, tra l'altro, dall'art. 9 del Patto internazionale sui diritti civili e politici e dall'art. 5 della Convenzione europea dei diritti umani.
[25] Si rimanda, tra gli altri, all'art. 14 del Patto internazionale sui diritti civili e politici e all'art. 6 della Convenzione europea dei diritti umani.
[26] Articolo 6 del Patto internazionale sui diritti civili e politici e articolo 2 della Convenzione europea dei diritti umani. Sul tema del ricorso ad armi autonome in attività di *law enforcement* si rinvia a A. Spagnolo, *What Do Human Rights Really Say About the Use of Autonomous Weapons Systems for Law Enforcement Purposes?*, in E. Carpanelli, N. Lazzerini (a cura di), *Use and Misuse of New Technologies. Contemporary Challenges in International and European Law*, Cham, 2019, 55-72.
[27] L. McGregor, D. Murray, Vivian Ng, *International Human Rights Law as a Framework for Algorithmic Accountability*, in *International & Comparative Law Quarterly*, 68, 2019, 327.
[28] *Ibid.* Come sottolineato dal Comitato dei Ministri del Consiglio d'Europa in una raccomandazione del 2020, «when algorithmic systems have the potential to create an adverse human rights impact for an individual, for a particular group or for the

DPCE online
ISSN: 2037-6677

sulla tutela dei diritti umani potrebbe permettere di superare i limiti connessi ad altri tentativi di garantire accountability, ad esempio attraverso il ricorso al principio di trasparenza[29].

Ma quali sono tali obblighi e come rilevano rispetto all'utilizzo dell'intelligenza artificiale per fini di polizia predittiva? Se è vero che gli stessi variano a seconda della natura del diritto e delle attività in esame, essi richiedono, in genere, l'adozione di misure, legislative e non, in grado di prevenire possibili violazioni, anche da parte di attori privati, la previsione di meccanismi di controllo contro possibili abusi, e la predisposizione di meccanismi che garantiscano alle vittime un rimedio effettivo. Non stupisce, pertanto, che il Comitato delle Nazioni Unite sull'eliminazione di ogni forma di discriminazione razziale abbia sottolineato come gli Stati contraenti che ricorrano alla profilazione algoritmica per fini, tra l'altro, di polizia predittiva debbano «adopt appropriate legislative, administrative and other measures to determine the purpose of their use and to regulate as accurately as possible the parameters and guarantees that prevent breaches of human rights. Such measures should, in particular, be aimed at ensuring that the deployment of algorithmic profiling systems does not undermine the right not to be discriminated against, the right to equality before the law, the right to liberty and security of person, the right to the presumption of innocence, the right to life, the right to privacy, freedom of movement, freedom of peaceful assembly and association, protections against arbitrary arrest and other interventions, and the right to an effective remedy»[30]. Inoltre, gli Stati contraenti devono «adopt measures to ensure that independent oversight bodies have a mandate to monitor the use of artificial intelligence tools by the public sector», «adopt measures to ensure that private sector design, deployment and implementation of artificial intelligence systems in the area of law enforcement comply with human rights standards», ed «ensure that all instances of algorithmic bias are duly investigated and that sanctions are imposed»[31].

Ne consegue che gli Stati che utilizzano o ammettono l'utilizzo di tecniche di polizia predittiva avranno l'obbligo di adottare misure volte a prevenire possibili violazioni dei diritti umani, ad esempio sottoponendo l'utilizzo di tali tecniche a una valutazione di impatto sulla tutela dei diritti umani o proibendo il loro utilizzo laddove sia tecnicamente impossibile eliminare l'impatto negativo sul godimento dei diritti fondamentali.

population at large, including effects on democratic processes or the rule of law, these impacts engage State obligations and private sectors responsibilities with regard to human rights». Si rinvia a Raccomandazione del Comitato dei Ministri del Consiglio d'Europa su *the human rights impacts of algorithmic systems*, doc. CM/Rec(2020)1, 8 aprile 2020.

[29] L. McGregor, D. Murray, Vivian Ng, *International Human Rights Law as a Framework for Algorithmic Accountability*, cit., 320 ss.

[30] Si rinvia nuovamente a Raccomandazione generale n. 36(2020) on preventing and combating racial profiling by law enforcement officials, cit., par. 59.

[31] *Ibid.*, parr. 62, 63 e 65.

Dovranno, inoltre, prevedere meccanismi indipendenti di controllo, che monitorino costantemente il rischio di violazioni connesso all'utilizzo di tali tecniche sia da parte delle forze di polizia sia da parte di soggetti privati che utilizzino tali tecniche per conto delle autorità di pubblica sicurezza. Infine, dovranno garantire che, laddove un individuo subisca una violazione dei propri diritti quale conseguenza del ricorso a tecniche di polizia predittiva, lo stesso abbia a sua disposizione meccanismi per ottenere un rimedio effettivo.

2.2. La proposta di regolamento dell'Unione europea in materia di intelligenza artificiale

Alla luce delle osservazioni contenute nel paragrafo precedente, è possibile svolgere alcune brevi riflessioni preliminari sulla proposta di regolamento del Parlamento europeo e del Consiglio in materia di intelligenza artificiale[32], che, se adottata, stabilirà vincoli uniformi per gli Stati membri.

Tale proposta, il cui obiettivo è, tra l'altro, di assicurare che i sistemi di intelligenza artificiale immessi sul mercato dell'Unione rispettino la normativa vigente in materia di diritti fondamentali e i valori dell'Unione[33], inserisce i sistemi di polizia predittiva tra quelli ad alto rischio, ossia quei sistemi che pongono rischi significativi per i diritti fondamentali. In base all'art. 6 dell'Allegato III, infatti, rientrano tra i sistemi ad alto rischio: «(a) AI systems intended to be used by law enforcement authorities for making individual risk assessments of natural persons in order to assess the risk of a natural person for offending or reoffending or the risk for potential victims of criminal offences; …(e) AI systems intended to be used by law enforcement authorities for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 or assessing personality traits and characteristics or past criminal behaviour of natural persons or groups; (f) AI systems intended to be used by law enforcement authorities for profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of detection, investigation or prosecution of criminal offences; (g) AI systems intended to be used for crime analytics regarding natural persons, allowing law enforcement authorities to search complex related and unrelated large data sets available in different

[32] Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale e modifica alcuni atti legislativi dell'Unione europea, 21 aprile 2021. Per un commento si rinvia, tra gli altri, a C. Casonato, B. Marchetti, *Prime Osservazioni sulla proposta di Regolamento dell'Unione europea in materia di intelligenza artificiale*, in *BioLaw Journal – Rivista di BioDiritto*, 3, 2021, 1-29. A questo proposito, si veda in questo fascicolo anche B. Marchetti, L. Parona, *La regolazione dell'intelligenza artificiale: Stati Uniti e Unione europea alla ricerca di un possibile equilibrio.*

[33] *Ibid.*, nella sezione "Contesto della proposta".

DPCE online
ISSN: 2037-6677

data sources or in different data formats in order to identify unknown patterns or discover hidden relationships in the data».

Tra i sistemi proibiti, in quanto comportanti un rischio inaccettabile, figurano, invece, i sistemi di valutazione e classificazione dell'affidabilità delle persone fisiche e, salvo alcuni casi eccezionali, i sistemi di identificazione biometrica remota "in tempo reale"[34].

Per essere immessi nel mercato dell'Unione, i sistemi ad alto rischio dovranno rispettare una serie di requisiti (ad esempio, in termini di trasparenza, sorveglianza umana, accuratezza e cibersicurezza) e superare una procedura di valutazione di conformità[35]. Inoltre, le autorità di vigilanza del mercato indagheranno in merito al rispetto degli obblighi e dei requisiti per tutti i sistemi di intelligenza artificiale ad alto rischio già immessi sul mercato[36]. Ciò al fine di minimizzare i rischi legati all'utilizzo di tali sistemi. Tuttavia, come specificato nella proposta di regolamento, nel caso in cui si verificassero comunque violazioni dei diritti fondamentali, un ricorso effettivo a favore delle vittime sarebbe reso possibile dalla trasparenza e dalla tracciabilità dei sistemi di intelligenza artificiale e dai controlli successivi[37].

Il quadro normativo delineato dalla proposta sembra muoversi, in linea di principio, nella direzione della prevenzione di possibili violazioni dei diritti umani, contestualmente ravvisando forme di monitoraggio successivo e favorendo l'esercizio del diritto a un rimedio effettivo laddove il godimento di alcuni diritti sia limitato. Tuttavia, è stato osservato come la vaghezza di alcuni termini, l'assenza di una valutazione di impatto sui diritti umani come requisito per i sistemi ad alto rischio, nonché il ruolo preponderante dei fornitori dei sistemi nei controlli successivi favorirebbero l'utilizzo, da parte delle forze di polizia, di tecniche predittive incompatibili con la tutela dei diritti umani[38]. In effetti, se è vero che alcuni rischi di violazione dei diritti umani potrebbero essere evitati attraverso interventi nella fase di realizzazione di un determinato sistema, è dubbio se i requisiti previsti nella proposta di regolamento siano sufficienti, in concreto, ad eliminarli.

È peraltro opportuno rilevare come il Parlamento europeo, nella già richiamata risoluzione del 6 ottobre 2021 in materia di intelligenza artificiale nel diritto penale, sembri aver dato seguito a tale perplessità, di fatto opponendosi al ricorso a tecniche di polizia predittiva. Rimane da vedere se e, nel caso, in che misura tale approccio restrittivo avrà un impatto in sede di adozione della proposta di regolamento.

[34] *Ibid.*, art. 5.
[35] *Ibid.*, art. 6 ss. e art. 19.
[36] *Ibid.*, art. 63.
[37] *Ibid.*, par. 3.5, "Diritti fondamentali".
[38] S. Kloving Skelton, *NGO Fair Trials Call on EU to Ban Predictive Policing Systems*, in *ComputerWeekly.com*, 20 settembre 2021.

3. L'utilizzo di algoritmi predittivi nel contesto di operazioni militari

Il dibattito concernente il ricorso all'intelligenza artificiale nel contesto dei conflitti armati si è finora concentrato principalmente sullo sviluppo e sull'utilizzo di armi autonome[39]. Al contrario, il ricorso ad algoritmi predittivi in contesti militari ha ricevuto scarsa attenzione.

Tuttavia, come già rilevato nell'introduzione, la prassi recente segnala un interesse crescente nei confronti dell'impiego di tali tecnologie in operazioni militari, soprattutto per programmare attacchi e valutare l'opportunità di un prolungamento della detenzione dei combattenti nemici.

Il ricorso ad algoritmi predittivi durante le ostilità si caratterizza per possibili profili di incompatibilità sia con le norme sui diritti umani sia con il diritto umanitario, stante l'applicazione contestuale di queste due branche del diritto internazionale nel contesto dei conflitti armati. Per quanto concerne la tutela dei diritti umani, il ricorso ad algoritmi predittivi in contesti militari, per fini di detenzione o *targeting*, comporterebbe un rischio di violazione di numerosi diritti, già richiamati in precedenza, tra cui: il diritto a non subire discriminazioni, il diritto alla vita (in caso di operazioni di *targeting*) e il diritto alla libertà personale (laddove il ricorso ad algoritmi predittivi avesse un impatto sulla detenzione dei combattenti nemici). Peraltro, in contesti militari, il rischio di simili violazioni potrebbe talora risultare accentuato. Ad esempio, il rischio di discriminazioni potrebbe essere esacerbato laddove, nel programmare il sistema, non si tenesse conto delle usanze culturali dei combattenti nemici[40].

Nella prospettiva del diritto umanitario, il ricorso a simili algoritmi predittivi, laddove finalizzato a programmare attacchi e in mancanza di una sorveglianza umana, rischierebbe, invece, di determinare una violazione di alcuni principi fondamentali che disciplinano i conflitti armati, come i principi di proporzionalità e distinzione[41].

Anche con riferimento a tali applicazioni dell'intelligenza artificiale è stato sottolineato, peraltro, come le norme internazionali potrebbero facilitare la definizione di un "accountability framework", che dovrebbe precedere il loro utilizzo[42]. Tuttavia, l'utilizzo di algoritmi predittivi in contesti militari sembra porre sfide ulteriori rispetto a quelle legate al ricorso alle medesime tecniche per finalità di polizia predittiva. A mero titolo esemplificativo, basti menzionare come la segretezza che generalmente caratterizza le operazioni militari e la localizzazione delle condotte in Stati

[39] Si rinvia, ex multis, a D. Amoroso, *Autonomous Weapons Systems and International Law. A Study on Human-Machine Interactions in Ethically and Legally Sensitive Domains*, Napoli, 2020. Si veda anche, più recentemente, T. Vestner, A. Rossi, *Legal Review of War Algorithms*, in *International Law Studies*, 97, 2021, 509-555.
[40] Si rimanda nuovamente a A. S. Deeks, *Predicting Enemies*, cit., 1567.
[41] Su questi principi di diritto umanitario si rinvia, tra gli altri, a M. Fornari, *Nozioni di diritto internazionale dei conflitti armati*, Napoli, 2015, 155 ss.
[42] Si veda L. McGregor, *The Need for Clear Governance Framework on Predictive Algorithms in Military Settings*, in *Humanitarian Law & Policy*, 28 marzo 2019.

DPCE online
ISSN: 2037-6677

stranieri potrebbero ostacolare la previsione di meccanismi indipendenti di controllo e l'esercizio del diritto a un rimedio effettivo da parte delle vittime[43].

È evidente, tuttavia, come la creazione di un quadro giuridico ad hoc sul piano internazionale, che garantisca un ricorso ad algoritmi predittivi compatibile con le norme esistenti, debba necessariamente ovviare alle criticità sopra esposte.

Elena Carpanelli
Dip.to di Giurisprudenza, St. pol. e internaz.
Università degli Studi di Parma
elena.carpanelli@unipr.it

[43] A. S. Deeks, *Predicting Enemies*, cit., 1573.