



Assemblea Generale

Distr.: Generale
14 luglio 2025

Originale: inglese

Consiglio per i diritti umani

Sessantesima sessione

8 settembre–3 ottobre 2025

Punti 3 e 5 dell'ordine del giorno

Promozione e protezione di tutti i diritti umani, civili, politici,
economici, sociali e culturali, compreso il
diritto allo sviluppo

Organi e meccanismi per i diritti umani

Implicazioni per i diritti umani delle tecnologie nuove ed emergenti nel settore militare

Rapporto del Comitato consultivo del Consiglio per i diritti umani



I. Introduzione

A. Mandato

1. Il presente rapporto è previsto dal mandato conferito dal Consiglio per i diritti umani con la risoluzione 51/22, nella quale è stato richiesto al Comitato consultivo del Consiglio per i diritti umani di preparare uno studio volto a esaminare le implicazioni per i diritti umani delle tecnologie nuove ed emergenti nel settore militare.

2. In occasione della sua ventinovesima sessione, il Comitato consultivo ha istituito un gruppo di redazione composto da Buhm-Suk Baek (Presidente), Nadia Amal Bernoussi, Milena Costas Trascasas, Alessandra Devulsky, Jewel Major, Javier Palummo (Relatore), Vasilka Sancin, Vassilis Tzevelekos, Catherine Van de Heyning, Frans Viljoen e Yue Zhang.

B. Ambito dello studio

3. Nel presente studio, il Comitato consultivo prende in esame l'intero ciclo di vita delle tecnologie nuove ed emergenti nel settore militare. Esso esamina in che modo il diritto internazionale dei diritti umani informi i processi decisionali relativi alla raccolta dati e alla loro gestione, alla trasparenza, all'obbligo di rendere conto, alla non discriminazione e alla protezione dei diritti. Il documento delinea i quadri giuridici internazionali applicabili alla progettazione, allo sviluppo, all'impiego e alla supervisione di tali tecnologie e al loro potenziale a duplice uso (militare e civile).

4. Lo studio contiene un'analisi di come i trattati internazionali vigenti, il diritto internazionale consuetudinario e gli strumenti di soft law, tra cui i Principi guida su imprese e diritti umani, possano contribuire a regolamentare lo sviluppo e l'uso di tali tecnologie, nonché un esame della rilevanza e dei ruoli complementari del diritto internazionale umanitario e del diritto internazionale dei diritti umani.

5. Il testo esamina inoltre le implicazioni per i diritti umani delle tecnologie nuove ed emergenti nel settore militare, integrando i dibattiti in sede di Nazioni Unite, i contributi delle parti interessate, incluse 22 risposte ai questionari,¹ e ricerche secondarie volte ad analizzare lo stato attuale e le nascenti preoccupazioni in materia di diritti umani connesse alle tecnologie nuove ed emergenti nel settore militare. L'analisi adotta un approccio prospettico, prendendo in considerazione i potenziali scenari derivanti dalle nuove tecnologie. La sezione conclusiva dello studio contiene raccomandazioni per azioni future.

C. Quadro concettuale e normativo

1. Tecnologie nuove ed emergenti, settore militare e a duplice uso

6. Ai fini della presente relazione, per "settore militare" si intende l'ambiente operativo delle forze armate e le attività connesse alla difesa, incluse le forze di sicurezza. Le "tecnologie nuove ed emergenti" si riferiscono a quelle tecnologie in fase di sviluppo o di recente introduzione, spesso caratterizzate da un potenziale trasformativo. Essendo trainate da progressi in molteplici ambiti, segnatamente l'intelligenza artificiale (IA), le neuroscienze, la biotecnologia, la nanotecnologia e la robotica, le tecnologie nuove ed emergenti nel settore militare potrebbero non essere sempre sinonimo di "armi"; mentre alcune armi possono comportare l'impiego di tecnologie nuove ed emergenti, non tutte le tecnologie nuove ed emergenti nel settore militare sono armi. In virtù della loro natura a duplice uso, risulta complesso individuare tecnologie nuove ed emergenti nel settore militare che non risentano dell'innovazione, così come le innovazioni tecnologiche non possono essere circoscritte a un ambito puramente militare.² Le "tecnologie a duplice uso" si riferiscono a innovazioni dotate di applicazioni sia civili che militari, con il potenziale

¹ Cfr. <https://www.ohchr.org/en/hr-bodies/hrc/advisory-committee/human-rights-implications>.

² Si veda [international-conference_-military-technologies-vis-a-vis-human-rights-concerns_-summary-report.pdf](#).

utilizzi nei settori commerciale, pubblico e militare.³ Di conseguenza, il quadro concettuale del rapporto deve essere considerato flessibile, data la difficoltà di definire tali categorie con precisione.

7. Sebbene gli armamenti militari abbiano costantemente integrato nuove tecnologie, gli odierni progressi digitali, in particolare l'IA, rappresentano un significativo salto di qualità. Tale mutamento di paradigma si colloca in un contesto di divario tecnologico e asimmetria di potere, nel quale le tecnologie militari sviluppate in alcune aree geografiche possono essere dispiegate in Stati che esercitano un'influenza limitata sul loro sviluppo. Ad esempio, gli Stati del Sud globale sono spesso esclusi dallo sviluppo e dalla governance delle tecnologie nuove ed emergenti nel settore militare, nonostante le loro popolazioni possano essere colpite in misura sproporzionata dal loro impiego.

8. Le tecnologie nuove ed emergenti nel settore militare pongono sfide significative agli Stati e agli altri attori ai fini del rispetto del diritto internazionale dei diritti umani. Fondamentalmente, l'uso di tali tecnologie nel settore militare presenta il rischio di deumanizzare l'uso della forza, esacerbando tendenze che riducono le vite umane a meri dati attraverso la profilazione e l'acquisizione degli obiettivi algoritmiche, attenuando o persino escludendo le considerazioni morali ed etiche inerenti al giudizio umano⁴ e accrescendo il rischio di un uso della forza arbitrario e sproporzionato. Tale deumanizzazione risulta incompatibile con i principi dei diritti umani, tra cui il diritto alla vita, l'integrità personale, la non discriminazione e la dignità umana, pilastro del diritto internazionale dei diritti umani e di numerosi ordinamenti giuridici interni. Inoltre, le tecnologie nuove ed emergenti nel settore militare potrebbero produrre impatti differenziati sui diritti umani di gruppi distinti.⁵

9. Una questione centrale relativa alle tecnologie nuove ed emergenti nel settore militare concerne la misura in cui sia mantenuto un controllo umano significativo sulle tecnologie, in particolare su quelle che comportano l'uso della forza, inclusi i sistemi di armi autonome e altri sistemi armati privi di equipaggio. Tali tecnologie si fondano sull'automazione e su processi decisionali autonomi, determinando il rischio di una riduzione della supervisione umana e dell'obbligo di rendere conto. Le tecnologie nuove ed emergenti autonome nel settore militare possono dare adito a gravi violazioni dei diritti umani, incluse minacce ai diritti alla vita, alla libertà di espressione, al rispetto della vita privata e alla non discriminazione, nonché a violazioni del divieto di maltrattamenti. L'intero ciclo di vita di tali tecnologie deve conformarsi a un solido quadro di protezione dei diritti umani, assicurando che i progressi tecnologici non pregiudichino i diritti umani e che le vittime possano accedere ai meccanismi di accertamento della responsabilità e di riparazione.

10. Un'ulteriore sfida è costituita dal fatto che le tecnologie nuove ed emergenti nel settore militare – dai beni e componenti hardware al software – sono definite “tecnologie a duplice uso” e presentano il potenziale per essere impiegate nei settori commerciale, pubblico e militare. Considerate le potenziali lacune tra i quadri giuridici e la diffusione delle tecnologie nuove ed emergenti, le criticità emergenti relative ai diritti umani devono essere affrontate prima della loro fase operativa, segnatamente nei contesti di conflitto. I rischi risultano ulteriormente amplificati dal ruolo centrale ricoperto dal settore privato nello sviluppo delle tecnologie nuove ed emergenti. Le imprese, pertanto, rivestono un ruolo cruciale nella prevenzione di violazioni e abusi dei diritti umani.

2. Quadri giuridici internazionali applicabili all'intero ciclo di vita delle tecnologie nuove ed emergenti nel settore militare

11. Il diritto internazionale, sia di natura pattizia che consuetudinaria, si applica allo sviluppo e all'impiego di tecnologie nuove ed emergenti nel settore militare e gli Stati sono tenuti a conformarvisi. Gli Stati hanno, inoltre, l'obbligo positivo di assicurarne il rispetto qualora tali tecnologie siano utilizzate da attori non statali soggetti alla loro giurisdizione. L'intero ciclo di vita delle nuove

³ Marcello Ienca e Effy Vayena, “Dual use in the 21st century”, *Swiss Medical Weekly*, vol. 148, n. 4748 (2018); e Marcus Schulzke, “Drone proliferation and the challenge of regulating dual-use technologies”, *International Studies Review*, vol. 21, n. 3 (settembre 2019).

⁴ Christof Heyns, “Autonomous weapons in armed conflict and the right to a dignified life”, *South African Journal on Human Rights*, vol. 33, n. 1 (2017).

⁵ Si veda Conferenza internazionale della Croce Rossa e della Mezzaluna Rossa, risoluzione 34IC/24/R2.

e le tecnologie emergenti nel settore militare sono disciplinate da molteplici quadri giuridici internazionali, ⁶ che si applicano in modo complementare e sinergico. ⁷

12. Il diritto internazionale dei diritti umani svolge un ruolo cruciale nel disciplinare le tecnologie nuove ed emergenti nel settore militare e trova applicazione sia in tempo di pace che durante i conflitti armati. Taluni diritti umani sono inderogabili, anche in tempo di conflitto armato, ivi compresi il diritto alla vita, ⁸ il divieto di maltrattamenti, schiavitù e servitù, nonché i principi di legalità, di irretroattività e di libertà di pensiero, coscienza e religione. ⁹

13. I principali strumenti pertinenti alle tecnologie nuove ed emergenti nel settore militare includono la Carta internazionale dei diritti umani e i restanti trattati internazionali fondamentali in materia di diritti umani. Considerato il potenziale impiego delle tecnologie nuove ed emergenti per la sorveglianza di massa e per pratiche discriminatorie, i principi di trasparenza e l'obbligo di rendere conto risultano cruciali in tale ambito. I diritti al rispetto della vita privata, alla libertà di espressione e alla non discriminazione, unitamente a quelli relativi alla salute, alla cultura e al lavoro, devono essere garantiti nelle fasi di progettazione, sviluppo e impiego di tali tecnologie. Il divieto di maltrattamenti si estende parimenti al loro utilizzo. Il principio di non discriminazione assume una rilevanza particolare, poiché le tecnologie nuove ed emergenti possono amplificare le distorsioni a danno di gruppi emarginati o vulnerabili qualora gli algoritmi non siano correttamente progettati e monitorati. Gli Stati sono tenuti a garantire che lo sviluppo e l'impiego di tecnologie nuove ed emergenti nel settore militare siano conformi al diritto internazionale dei diritti umani e che siano predisposti ricorsi effettivi in caso di violazioni. Le imprese coinvolte nello sviluppo o nell'impiego di tali tecnologie sono tenute ad aderire ai pertinenti standard, in conformità con i Principi guida, a evitare violazioni dei diritti umani e a prevenire proattivamente potenziali rischi per i diritti umani nell'ambito delle pro-

14. Il diritto internazionale umanitario risulta altresì fondamentale per la regolamentazione delle tecnologie nuove ed emergenti nel settore militare. Mentre taluni trattati disciplinano o vietano esplicitamente armi specifiche, le Convenzioni di Ginevra e i relativi Protocolli aggiuntivi si applicano a ogni forma di conduzione delle ostilità e a ogni tipologia di armi, incluse quelle non ancora sviluppate, come confermato dalla Corte Internazionale di Giustizia. ¹⁰ L'articolo 36 del Protocollo aggiuntivo alle Convenzioni di Ginevra del 12 agosto 1949 relativo alla protezione delle vittime dei conflitti armati internazionali (Protocollo I) impone alle Parti l'obbligo di verificare se le nuove armi, i mezzi o i metodi di guerra studiati, sviluppati, acquisiti o adottati siano vietati dal Protocollo medesimo o da altre norme del diritto internazionale. Sebbene tale disposizione vincoli formalmente solo le Parti del suddetto Protocollo, anche alcuni Stati non aderenti procedono all'esame della legittimità giuridica delle armi.

15. La Convenzione sulla proibizione o la limitazione dell'impiego di talune armi classiche che possono essere ritenute capaci di causare effetti traumatici eccessivi o di colpire in modo indiscriminato mira a vietare e limitare l'uso di determinati tipi di armi che sono considerate causa di sofferenze non necessarie o ingiustificabili ai combattenti o tali da colpire i civili in modo indiscriminato. I Protocolli alla Convenzione disciplinano l'uso di armi specifiche e lo sviluppo di tecnologie belliche applicando tre principi fondamentali del diritto internazionale umanitario: (a) il diritto delle Parti di un conflitto armato di scegliere metodi o mezzi di guerra non è illimitato; (b) la protezione della popolazione civile contro gli effetti delle ostilità; e (c) il divieto di causare lesioni superflue o sofferenze non necessarie ai combattenti. Inoltre, il Gruppo di esperti governativi sulle tecnologie emergenti nell'ambito dei sistemi di armi autonome letali ha ribadito che il diritto internazionale umanitario continua ad applicarsi integralmente al potenziale sviluppo e all'impiego di sistemi di armi autonome letali. ¹¹

16. Il diritto internazionale umanitario rimane essenziale per la protezione dei civili dagli effetti dei conflitti armati a fronte del rapido progresso tecnologico, ponendo tale onere in capo agli Stati

⁶ Ciò include altri ambiti del diritto internazionale (ad es. il diritto ambientale e del lavoro). Gruppi di Stati hanno inoltre adottato dichiarazioni, impegni e codici di condotta pertinenti.

⁷ *International Legal Protection of Human Rights in Armed Conflict* (Pubblicazione delle Nazioni Unite, 2011). Si veda anche la risoluzione 51/22 del Consiglio per i diritti umani.

⁸ Si veda Comitato per i diritti umani, commento generale n. 36 (2018).

⁹ Si veda Comitato per i diritti umani, commento generale n. 29 (2001).

¹⁰ *Legality of the Threat or Use of Nuclear Weapons*, *Parere consultivo*, I.C.J. Reports 1996, p. 226, par. 86.

¹¹ CCW/GGE.1/2023/2, par. 21 (a).

per garantire la conformità, indipendentemente dai progressi scientifici e tecnologici.¹² Anche qualora gli Stati non siano parti dei trattati summenzionati, essi rimangono vincolati dal diritto internazionale consuetudinario, di cui diverse norme hanno natura di *jus cogens*. Gli Stati devono altresì ottemperare ai propri obblighi di dovuta diligenza, il che impone di approfondire ogni sforzo volto a prevenire la violazione di un obbligo internazionale, segnatamente mediante l'adozione di normative e misure, nonché l'adempimento del dovere di vigilanza applicabile a soggetti pubblici e privati.¹³ Si osserva, in particolare, che la dovuta diligenza costituisce un obbligo di mezzi e non di risultato.

17. L'obbligo di garantire che gli sviluppi di tecnologie nuove ed emergenti nel settore militare non violino il Diritto internazionale rappresenta un obbligo primario in capo a ciascuno Stato.¹⁴

Pertanto, gli Stati sono tenuti a condurre valutazioni approfondite al fine di determinare le modalità di applicazione di specifiche norme giuridiche internazionali alle tecnologie nuove ed emergenti nel settore militare. A questo proposito, le istituzioni nazionali per i diritti umani devono rivestire un ruolo di rilievo.¹⁵ La revisione tempestiva della legislazione interna di ciascuno Stato è essenziale per individuare e risolvere eventuali discrepanze rispetto alle norme internazionali.

18. Nonostante i quadri giuridici vigenti, il rapido progresso delle tecnologie nuove ed emergenti nel settore militare ne ostacola l'effettiva attuazione. Tale scenario ha alimentato il dibattito in merito all'applicazione del Diritto internazionale alle tecnologie nuove ed emergenti nel settore militare, inclusi i processi decisionali basati sull'IA, i sistemi di armi autonome, i sistemi senza equipaggio e i programmi militari intesi a potenziare le capacità fisiche e cognitive dei combattenti.

Sebbene l'IA e le tecnologie nuove ed emergenti introducano nuovi termini, le parti interessate devono garantire la coerenza con il linguaggio e gli standard giuridici internazionali.¹⁶

II. Impatto sui diritti umani

A. L'intelligenza artificiale quale tecnologia abilitante nel settore militare

19. Nel settore militare, l'IA funge da tecnologia abilitante fondamentale, potenziando le capacità operative in diverse funzioni. Occorre distinguere tra le tecnologie basate sull'IA – strumenti e sistemi che utilizzano l'IA a supporto del processo decisionale umano – e i sistemi autonomi, quali i sistemi di armi autonome, in grado di operare con un intervento umano limitato o nullo. Sebbene l'IA possa fornire ausilio al processo decisionale, non tutti i sistemi basati sull'IA sono autonomi, né l'autonomia implica intrinsecamente l'uso dell'IA. La presente sezione esamina il ruolo dell'IA quale strumento di potenziamento sotto la supervisione umana.

20. Sebbene l'IA sia oggetto di sviluppo da decenni e possa essere considerata una tecnologia emergente di lunga data, il suo ruolo nel potenziare l'autonomia dei sistemi di armi, nel sostenere il processo decisionale in ambito militare e nell'integrarsi nelle catene di approvvigionamento militari ha assunto recentemente una rilevanza primaria. I recenti progressi nel campo dell'informatica hanno accresciuto il ruolo dell'IA in tali ambiti.¹⁷ 21. L'IA è sempre più inte-

grata nelle operazioni militari e impiegata per potenziare l'analisi dell'intelligence, la pianificazione degli scenari, la logistica e i processi decisionali sul campo di battaglia. I sistemi di IA possono operare con vari gradi di autonomia: si osserva che a una maggiore autonomia corrisponde una minore supervisione umana e un minore controllo. L'IA può coadiuvare il processo decisionale attraverso, ad esempio, l'elaborazione rapida di vaste quantità di dati e può potenzialmente prevalere sul giudizio umano in specifici scenari prestabiliti, quali le situazioni di alta pressione. Tuttavia, l'IA solleva altresì preoccupazioni in materia di diritti umani, in particolare con riferimento alla libertà di espressione, al rispetto della vita privata e alla non discriminazione. Ad esempio, essa potrebbe erroneamente identificare un dispositivo di assistenza per la disabilità come un'arma, violando il principio di non discriminazione.

¹² Il diritto pattizio è parimenti applicabile a tale riguardo (ad esempio, il Protocollo I addizionale alle Convenzioni di Ginevra del 1949).

¹³ Corte Internazionale di Giustizia, *Cartiere sul fiume Uruguay (Argentina c. Uruguay)*, Sentenza, I.C.J. Reports 2010, p. 14, par. 197.

¹⁴ Comitato Internazionale della Croce Rossa (ICRC), *Autonomous Weapon Systems: Implications of Increasing Autonomy in the Critical Functions of Weapons* (Ginevra, 2016).

¹⁵ Contributo della Digital Rights Alliance.

¹⁶ Si veda committees.parliament.uk/writtenevidence/120290/pdf/.

¹⁷ Steffa Schmid, Thea Riebe e Christian Reuter, "Dual-use and trustworthy?", *Science and Engineering Ethics*, vol. 28, n. 2 (marzo 2022).

principi.¹⁸ I pregiudizi algoritmici possono altresì condurre a forme di discriminazione razziale o di genere. Il rispetto della dignità umana, come prescritto dal diritto internazionale dei diritti umani, è essenziale durante l'intero ciclo di vita dell'IA al fine di garantire l'eguale valore di ogni individuo.¹⁹

22. L'IA può limitare la supervisione umana e la capacità di esercitare un giudizio morale o giuridico in merito ai risultati da essa generati. La sfida cruciale consiste nel determinare se, e in quale misura, il diritto internazionale richieda il controllo umano nelle procedure di acquisizione degli obiettivi, nella detenzione, nell'impiego delle armi e nella salvaguardia della dignità umana. Ciò include la conformità a quadri giuridici quali la Dichiarazione universale dei diritti umani, la quale stabilisce che tutti gli esseri umani sono «dotati di ragione e di coscienza e devono agire gli uni verso gli altri in spirito di fratellanza».

23. Un'altra questione cruciale è la mancanza di trasparenza nei processi decisionali dell'IA, con numerosi sistemi che operano come «scatole nere», ponendo una sfida ai principi dei diritti umani in materia di trasparenza e ricorso effettivo. I quadri di responsabilità vigenti, basati sull'azione umana, potrebbero essere messi a rischio dall'integrazione dell'IA, in particolare nel caso dell'apprendimento automatico. Garantire linee di responsabilità chiare è essenziale, ma risulta problematico quando l'IA opera con una significativa autonomia o quando il suo ragionamento è opaco. L'obbligo di rendere conto include sia misure preventive sia valutazioni ex post di potenziali violazioni del Diritto internazionale. I principali meccanismi di accertamento della responsabilità si applicano sia alla responsabilità penale individuale sia alla responsabilità dello Stato.

24. Sotto il profilo dei diritti umani, desta inoltre preoccupazione il fatto che le tecnologie nuove ed emergenti nel settore militare, in particolare quelle basate sull'IA, consumino elevate quantità di energia, generino significative emissioni di carbonio e dipendano fortemente da materie prime quali nichel, cobalto e grafite, comportando rischi a lungo termine, anche per il diritto a un ambiente pulito, sano e sostenibile. Con l'evolversi di tali tecnologie, appare essenziale affrontarne le ripercussioni sui diritti umani e sull'ambiente.

B. Sistemi di armi autonome e relative implicazioni per l'agenzia umana e l'obbligo di rendere conto

25. I sistemi di armi autonome sono in grado di adottare decisioni indipendenti con un intervento umano limitato o nullo. I sistemi di armi autonome letali, sottocategoria dei sistemi di armi autonome, si distinguono per la capacità di eseguire autonomamente decisioni che possono comportare l'impiego della forza letale. La definizione dei sistemi di armi autonome costituisce una sfida giuridica, in ragione dei diversi livelli possibili di intervento e controllo umano. L'assenza di consenso tra gli Stati in merito a tale definizione giuridica ne complica ulteriormente la regolamentazione.²⁰

26. Diversamente dai sistemi decisionali automatizzati che operano sulla base di comandi e criteri predefiniti, i sistemi di armi autonome sono concepiti per operare con livelli superiori di autonomia, sollevando complessi interrogativi giuridici circa la loro conformità al diritto internazionale. Tali sistemi presentano, ad esempio, sfide peculiari in materia di dignità umana, controllo umano e trasparenza, con ripercussioni sui diritti alla vita, a un ricorso effettivo e al rispetto della vita privata.²¹ Nell'ambito del diritto internazionale umanitario, le principali criticità attengono ai principi di distinzione, proporzionalità, precauzione nell'attacco e all'obbligo di condurre un esame della liceità delle armi.

27. I sostenitori di un divieto dei sistemi di armi autonome sostengono che tali sistemi potrebbero violare la clausola Martens della Convenzione per il regolamento pacifico delle controversie internazionali, in base alla quale le armi devono essere conformi ai «principi di umanità e ai dettami della coscienza pubblica».²² Tuttavia, essi spesso considerano tale clausola come base per la regolamentazione piuttosto

¹⁸ A/HRC/49/52, par. 54.

¹⁹ Organizzazione delle Nazioni Unite per l'Educazione, la Scienza e la Cultura, Raccomandazione sull'etica dell'intelligenza artificiale.

²⁰ Si veda [https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-_Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_\(2023\)/CCW_GGE1_2023_CRP.1_0.pdf](https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-_Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2023)/CCW_GGE1_2023_CRP.1_0.pdf).

²¹ Documento presentato da Privacy International.

²² Rupert Ticehurst, «The Martens clause and the laws of armed conflict», *International Review of the Red Cross*, n. 317, aprile 1997.

piuttosto che un divieto.²³ Al contrario, gli oppositori di un divieto potrebbero persino mettere in dubbio il valore giuridico di tale clausola.²⁴

28. Nonostante il consenso in merito alla necessità di mantenere il controllo umano sui sistemi di armi autonome, si riscontra una carenza di normative e standard internazionali specifici volti a garantire un controllo umano significativo sull'uso della forza.²⁵ Diverse proposte hanno individuato elementi pratici del controllo umano, incluse limitazioni relative ai parametri d'uso e all'ambiente operativo. Misure quali la limitazione degli obiettivi, la supervisione umana obbligatoria e i meccanismi di accertamento della responsabilità sono state suggerite per far fronte all'imprevedibilità intrinseca e ai rischi derivanti dallo sviluppo, dall'impiego e dall'uso di tali sistemi.²⁶ In seno al Gruppo di esperti governativi, il cui mandato include sia le tecnologie autonome che l'IA, è tuttora in corso il dibattito su cosa costituisca un "controllo umano significativo". Tuttavia, non è stato ancora raggiunto un consenso al riguardo. Ciononostante, sussiste un ampio accordo sulla necessità di mantenere un certo grado di coinvolgimento umano. Inoltre, la questione dei diritti umani rimane ampiamente esclusa dalle discussioni del Gruppo di esperti governativi.²⁷

29. L'integrazione dell'IA e delle tecnologie autonome in tali nuovi sistemi presenta sfide giuridiche internazionali peculiari. Nel quadro dell'attuale regime giuridico, l'impiego dell'IA può complicare la determinazione della responsabilità e dell'obbligo di rendere conto per le violazioni del Diritto internazionale. La ridotta trasparenza nell'acquisizione degli obiettivi basata sull'IA può generare lacune, rendendo più ardua l'attribuzione della responsabilità penale individuale per crimini di guerra o della responsabilità dello Stato per violazioni del Diritto internazionale. Sebbene la responsabilità penale individuale sia stata ampiamente dibattuta in dottrina e in seno alle Nazioni Unite, le discussioni concernenti le sfide poste dai sistemi di armi autonome alla responsabilità dello Stato sono ancora in una fase iniziale.²⁸ Nel definire l'obbligo di rendere conto, occorre delineare le responsabilità specifiche degli sviluppatori tecnologici, degli operatori e dei comandanti militari, nonché gli obblighi dello Stato ai sensi del Diritto internazionale, inclusi i Principi guida. Una maggiore chiarezza giuridica su tali aspetti permane fondamentale, in quanto ogni tecnologia nuova ed emergente presenta sfide uniche ai diversi livelli di responsabilità.

30. Inoltre, l'attribuzione della condotta ai fini dell'accertamento della responsabilità dello Stato ai sensi del Diritto internazionale, nel contesto dei sistemi di armi autonome, solleva questioni giuridiche critiche che richiedono un esame approfondito. Sebbene gli Stati in seno al Gruppo di esperti governativi abbiano convenuto per consenso che ogni atto internazionalmente illecito di uno Stato, compresi quelli che potrebbero comportare l'impiego di sistemi di armi autonome letali, comporti la responsabilità internazionale dello Stato, non è stata fornita ulteriore chiarezza in merito all'attribuzione della responsabilità dello Stato per violazioni del Diritto internazionale.²⁹ Nella prima bozza di proposta della Presidenza è stato rilevato che la condotta degli organi di uno Stato – quali i suoi agenti e tutto il personale facente parte delle sue forze armate – è attribuibile a tale Stato, inclusi gli atti e le omissioni derivanti dall'uso di tali sistemi

²³ Si veda <https://blogs.icrc.org/law-and-policy/2017/11/14/ethics-source-law-martens-clause-autonomous-weapons/>.

²⁴ Paul Scharre, *Army of None: Autonomous Weapons and the Future of War* (New York, W.W. Norton & Company, 2018).

²⁵ Si veda <https://www.ejiltalk.org/what-level-of-human-control-over-autonomous-weapon-systems-is-required-by-international-law/>.

²⁶ Ibidem; Vincent Boulanin e altri, *Limits on Autonomy in Weapon Systems* (Stoccolma, Stockholm International Peace Research Institute e Comitato Internazionale della Croce Rossa, 2020); e CCW/GGE.1/2023/WP.6.

²⁷ Si veda CCW/GGE.1/2020/WP.6, CCW/GGE.1/2023/WP.2/Rev.1 e CCW/GGE.1/2024/WP.10.

²⁸ Robin Geiß, "State control over the use of autonomous weapon systems", in *Military Operations and the Notion of Control Under International Law*, Rogier Bartels e altri, a cura di (L'Aia, Asser Press, 2021); e Lutiana Valadares Fernandes Barbosa, *Sistemi di armi autonome e la responsabilità degli Stati: sfide e possibilità* (Boca Raton, Florida, Stati Uniti d'America, e Abingdon, Regno Unito di Gran Bretagna e Irlanda del Nord, CRC Press, 2024).

²⁹ CCW/GGE.1/2022/2, par. 19.

³⁰ Si veda <https://documents.unoda.org/wp-content/uploads/2022/07/CCW-GGE.1-2022-CRP.1.docx>. Si veda altresì CCW/GGE.1/2022/WP.2; e Alisha Anand Ioana Puscas, "Proposals related to emerging technologies in lethal autonomous weapons systems" (Istituto delle Nazioni Unite per la ricerca sul disarmo, 2022).

31. Una considerazione fondamentale riguarda se, e in quali circostanze, la condotta dei sistemi di armi autonome possa o debba essere attribuita allo Stato e se l'attuale regime sulla responsabilità internazionale degli Stati, basato su un paradigma di azione umana, sia sufficiente per attribuire la responsabilità nel contesto di tali sistemi.³¹ Sebbene gli Stati abbiano obblighi positivi in materia di diritti umani volti a garantire che tali tecnologie siano conformi al Diritto internazionale e ad adottare misure preventive per ridurre al minimo i rischi, il quadro degli obblighi positivi potrebbe non essere di per sé sufficiente a stabilire la responsabilità dello Stato nei casi in cui i sistemi di armi autonome operino con un'autonomia significativa e oltre la prevedibilità del supervisore umano. La sfida risiede nel determinare in quali circostanze le azioni compiute nel contesto di tali sistemi debbano essere assimilate alla condotta dello Stato che ne dispone l'impiego, impegnando così la responsabilità dello Stato per tali atti ai sensi del diritto internazionale. La risoluzione di tali questioni è essenziale per garantire l'obbligo di rendere conto e la conformità al diritto internazionale. 32. L'integrazione di capacità autonome nei sistemi di

armi dotati di tecnologia di IA introduce sfide peculiari nell'ambito degli esami di legittimità giuridica. I sistemi di armi autonome interagiscono con l'ambiente circostante, il che richiede l'esecuzione di test in una pluralità di scenari. A fronte del crescente affidamento umano sull'IA, deve essere rivolta maggiore attenzione alla compatibilità di tali sistemi con le norme giuridiche. Sebbene la selezione e la revisione dei dati algoritmici rappresentino componenti essenziali, un esame di legittimità giuridica completo dei sistemi di armi autonome che incorporano sistemi di IA dovrebbe tenere conto degli obblighi degli Stati ai sensi del diritto internazionale dei diritti umani, inclusi i diritti alla vita, all'integrità, alla non discriminazione e al rispetto della vita privata, nonché dei principi di trasparenza e dell'obbligo di rendere conto e dei potenziali rischi di conseguenze non intenzionali.³² Gli obblighi di dovuta diligenza dovrebbero essere definiti per eliminare distorsioni involontarie e discriminazioni, in particolare laddove queste possano violare diritti tutelati dal diritto internazionale. Gli esperti incaricati degli esami di legittimità devono essere coinvolti sin dalle fasi di progettazione per affrontare tali problematiche in modo proattivo e attuare misure di salvaguardia contro potenziali violazioni dei diritti umani. Nondimeno, permangono interrogativi circa la compatibilità dei processi decisionali automatizzati con i principi dei diritti umani,³³ ed è opportuno rilevare come sussista un considerevole dibattito sulla possibilità che i sistemi di armi autonome possano essere prodotti e impiegati in modo pienamente conforme a tutti i requisiti del diritto in-

33. L'avvento di tecnologie nuove ed emergenti nel settore militare, quali la tecnologia utilizzata nei sistemi di armi autonome, pone sfide al diritto internazionale vigente, evidenziando la necessità di nuove norme volte a regolamentare e, ove necessario, eventualmente proibire tali tecnologie qualora esse non siano in grado di soddisfare le norme giuridiche internazionali. Il Gruppo di esperti governativi sta esaminando un approccio articolato su due livelli, volto a proibire le armi incompatibili con il diritto internazionale umanitario e a regolamentare le restanti fattispecie. Tale orientamento è conforme agli appelli del Segretario Generale e del Presidente del Comitato Internazionale della Croce Rossa per l'adozione di nuove norme internazionali a salvaguardia dell'umanità.³⁴ Nella relazione redatta ai sensi della risoluzione 78/241 dell'Assemblea Generale, la prima risoluzione dell'Assemblea concernente i sistemi di armi autonome letali, il Segretario Generale ha esortato gli Stati a concludere, entro il 2026, uno strumento giuridicamente vincolante volto a proibire i sistemi che operano in assenza di controllo umano o supervisione e che non possono essere utilizzati in conformità con il diritto internazionale umanitario, nonché a regolamentare ogni altra tipologia di sistema di armi autonome.³⁵ Tuttavia, gli Stati rimangono divisi sulla natura, giuridicamente vincolante o volontaria, di tali regolamentazioni.³⁶ Risulta inoltre necessario un dibattito in merito al diritto internazionale dei diritti umani e ai sistemi di armi autonome

³¹ Articoli sulla responsabilità degli Stati per atti internazionalmente illeciti (*Annuario della Commissione del Diritto Internazionale* 2001, vol. II (Parte Seconda) (A/CN.4/SER.A/2001/Add.1 (Parte 2), p. 26); Rebecca Crootof, "War torts", *University of Pennsylvania Law Review*, vol. 164, n. 6 (maggio 2016); e Valadares Fernandes Barbosa, *Sistemi di armi autonome e la responsabilità degli Stati*.

³² Tobias Vestner e Altea Rossi, "Legal reviews of war algorithms", *International Law Studies*, vol. 97 (2021).

³³ Si veda A/HRC/23/47.

³⁴ Si veda <https://www.icrc.org/en/document/joint-call-un-and-icrc-establish-prohibitions-and-restrictions-autonomous-weapons-systems>.

³⁵ A/79/88, par. 90.

³⁶ Ibid., par. 63-86.

C. Tecnologie per il potenziamento umano nel settore militare

34. Nonostante il potenziale apporto a strategie non letali e alla riduzione dello stress nei conflitti, lo sviluppo di tecnologie di potenziamento fisico e cognitivo presenta significative sfide etiche, giuridiche, sociali e operative. Le criticità includono gli impatti sui valori militari, i dilemmi operativi, l'applicazione del diritto militare e il consenso informato. Inoltre, le diverse tipologie di potenziamento – genetico, biologico o cibernetico – comportano rischi distinti per i diritti umani e profili etici differenziati. Analoghi progressi in ambito civile, segnatamente nei contesti lavorativi, evidenziano le implicazioni più ampie e la natura a duplice uso di tali tecnologie.³⁷

35. I progressi nell'IA ampliano ulteriormente il potenziale delle tecnologie di potenziamento umano, rivestendo un ruolo cruciale nei trattamenti medici e nella riabilitazione di menomazioni fisiche e cognitive in contesti non militari.³⁸ Storicamente, le iniziative volte a potenziare le prestazioni umane hanno accordato priorità al successo della missione, talvolta a scapito del benessere individuale. Tale tensione può limitare l'autonomia dei soldati e dei medici militari nell'impiego di neurotecnologie (ad es. farmaci, impianti neurali o neuroprotesi). Garantire la trasparenza e il rispetto della dignità umana e del diritto alla salute risulta essenziale, ivi compresi l'autonomia decisionale e le condizioni post-servizio dei combattenti potenziati.³⁹

36. L'adozione di tecnologie quali le interfacce cervello-computer nel settore militare è ritenuta idonea a potenziare le capacità cognitive attraverso l'integrazione tra l'intelligenza umana e quella artificiale. Mentre lo sviluppo della robotica e delle neurotecnologie, quali le interfacce cervello-computer, presenta prospettive chiaramente significative nel settore sanitario, il loro impiego in ambito militare solleva sfide specifiche, segnatamente con riferimento all'applicazione delle norme disciplinanti l'obbligo di rendere conto e il controllo umano sulle operazioni militari e sui processi decisionali. Le interfacce cervello-computer e altre neurotecnologie avanzate potrebbero altresì prestarsi a usi impropri nell'ambito di tecniche di interrogatorio coercitivo in contesti conflittuali. L'impiego di siffatti metodi potrebbe configurare una violazione dei diritti umani, in quanto suscettibile di infliggere danni psicologici o di integrare il reato di tortura, pur in assenza di violenza fisica.⁴⁰

37. L'introduzione di nuove tecnologie di potenziamento umano nelle attività militari solleva gravi preoccupazioni circa le implicazioni giuridiche e i potenziali abusi dei diritti umani, in quanto esse comportano rischi relativi, in particolare, al rispetto della vita privata, alla necessità di acquisire il consenso libero e informato, nonché alle potenziali violazioni dell'integrità fisica e mentale dei combattenti nel lungo periodo. Gli Stati e le imprese hanno il dovere di affrontare tali rischi in conformità con le disposizioni applicabili del diritto internazionale.⁴¹

38. Inoltre, le asimmetrie di potere inerenti al settore militare, unitamente alle implicazioni a lungo termine delle pratiche di raccolta dati, trattamento e conservazione dei dati personali, possono determinare violazioni differite del rispetto della vita privata che si manifestano in una fase successiva. Ad esempio, l'uso coercitivo di tali tecnologie potrebbe compromettere gravemente la dignità e l'autonomia dei soldati, laddove le applicazioni non coercitive sollevano seri interrogativi etici riguardo al consenso e agli effetti sulla salute a lungo termine. Tali considerazioni dovrebbero indurre a prevedere divieti specifici in caso di uso coercitivo, nonché moratorie o limitazioni per gli usi non coercitivi, al fine di prevenire il potenziale abuso di tali tecnologie.⁴²

³⁷ Timo Istace e Milena Costas Trascasas, "Between science-fact and science-fiction", Research Brief (Ginevra, Geneva Academy of International Humanitarian Law and Human Rights, 2024).

³⁸ Yuval Shany e Tal Mimran, "Integrating privacy concerns in the development and introduction of new military or dual use technologies", in *The Rights to Privacy and Data Protection in Times of Armed Conflict*, Asaf Lubin e Russal Buchan, eds. (Talinn, NATO CCDCOE Publications, 2022); e Margaret Kosal e Joy Putney, "Neurotechnology and international security", *Politics and the Life Sciences*, vol. 42, n. 1 (primavera 2023).

³⁹ Sebastian Sattler e altri, "Neuroenhancements in the military" *Neuroethics*, vol. 15, n. 1 (febbraio 2022).

⁴⁰ Charles N. Munyon, "Neuroethics of non-primary brain computer interface", *Frontiers in Neuroscience* (ottobre 2018).

⁴¹ Cfr. [A/HRC/57/61](#).

⁴² Ibid., par. 80 (b).

D. Applicazione della legge e controllo delle frontiere

39. Tecnologie quali la sorveglianza basata sull'IA, la modellazione predittiva e la biometria sono sempre più utilizzate dalle autorità preposte al controllo delle frontiere e all'applicazione della legge. Sebbene tali strumenti siano spesso promossi per il loro potenziale nel migliorare la sicurezza pubblica, ottimizzando la risposta alle emergenze, consentendo attraversamenti sicuri e fluidi e assistendo nella prevenzione del crimine, essi pongono altresì gravi rischi per i diritti umani nei contesti di applicazione della legge e di controllo delle

frontiere.⁴³ 40. Le applicazioni biometriche in tale ambito comprendono la verifica dell'identità per il controllo degli accessi e l'identificazione durante la cattura o la detenzione. Sebbene tali sistemi siano suscettibili di errore, scarsa attenzione è stata dedicata alle potenziali ripercussioni sui diritti umani derivanti dal loro impiego nel settore militare, con particolare riferimento ai gruppi vulnerabili, quali le persone con disabilità, le persone anziane, i minori, le persone di discendenza africana, i migranti e altri soggetti colpiti da forme di discriminazione storica e strutturale. Sussiste il timore che la loro applicazione possa consolidare le disparità attraverso distorsioni e profilazioni discriminatorie, spesso derivanti da pregiudizi radicati nelle prassi storiche di raccolta dati, trattamento e conservazione. Nella gestione delle migrazioni, l'eterogeneità dei dati biometrici influenzata dalle differenze culturali può esacerbare tali distorsioni. A titolo esemplificativo, le tecnologie biometriche quali il riconoscimento facciale potrebbero violare il diritto alla non discriminazione, essendo inclini a identificare erroneamente i Popoli indigeni e le persone di discendenza africana, in particolare le donne. Tali tecnologie possono altresì ledere il diritto al rispetto della vita privata qualora i governi e le imprese condividano dati biometrici in assenza del consenso dell'interessato. Considerata la rilevanza attribuita dal diritto internazionale dei diritti umani al diritto esplicito al rispetto della vita privata, all'uguaglianza e alla non discriminazione, risulta essenziale condurre valutazioni d'impatto sui diritti umani e analizzare le modalità con cui tali tecnologie possano rafforzare le disuguaglianze pre-

41. I sistemi di sorveglianza ottica, compresa la sorveglianza aerea, dispongono attualmente di capacità senza precedenti per monitorare, registrare e tracciare a distanza individui in spazi pubblici, incluse le zone di frontiera, avvalendosi di tecnologie quali i droni e il riconoscimento facciale. Tali progressi pongono gravi rischi per i diritti umani, comprese le libertà di movimento, di associazione, di riunione, il rispetto della vita privata e la non discriminazione.

42. Negli ultimi anni, è stata rivolta una crescente attenzione ai sistemi di armi autonome. Sebbene gran parte del dibattito si sia concentrata sul loro impiego nei conflitti armati, appare sempre più evidente come tali sistemi siano presi in considerazione anche per la gestione delle frontiere e per l'applicazione della legge a livello nazionale. Tale spostamento solleva significative preoccupazioni in materia di diritti umani, in particolare per quanto riguarda i diritti alla vita, l'integrità fisica e la dignità. A differenza del conflitto armato, in cui l'uso della forza è disciplinato principalmente dal diritto internazionale umanitario, il personale addetto all'applicazione della legge può ricorrere alla forza solo qualora risulti inevitabile, strettamente necessario e proporzionato all'assolvimento dei propri doveri.⁴⁵

E. Guerra cognitiva

43. La guerra cognitiva mira al controllo dei pensieri e delle percezioni di un avversario al fine di influenzarne decisioni e azioni.⁴⁶ Radicata nella disinformazione militare, essa rappresenta una nuova frontiera strategica in virtù dell'impatto trasformativo dell'IA. Le tecnologie avanzate consentono un condizionamento psicologico su vasta scala, l'acquisizione degli obiettivi cognitivi in assenza di consapevolezza e l'incremento della precisione. Attraverso l'alterazione delle percezioni e lo sfruttamento delle vulnerabilità nei processi decisionali, essa garantisce vantaggi strategici.

44. Sebbene la guerra cognitiva non sia di per sé sufficiente per vincere i conflitti, la sua combinazione con operazioni fisiche e informative – quale la disinformazione basata sull'IA – può determinare la supremazia sull'avversario. I non combattenti, compresa la popolazione civile, sono sempre più esposti alle strategie di guerra cognitiva, il che solleva gravi preoccupazioni in merito alla tutela dei diritti umani in tale ambito. Tali tattiche potrebbero pregiudicare i diritti umani, tra cui il diritto al rispetto della vita privata attraverso la raccolta dati e la profilazione, nonché il diritto alla libertà di opinione e

⁴³ Matias Leese e altri, "Data matters", *Geopolitics*, vol. 27, n. 1 (2022).

⁴⁴ Cfr. [A/HRC/51/17](#).

⁴⁵ Codice di condotta per i funzionari responsabili dell'applicazione della legge.

⁴⁶ Jean-Marc Rickli, Federico Mantellassi e Gwyn Glasser, "Peace of mind", Policy Brief n. 9 (Ginevra, Geneva Centre for Security Policy, 2023).

espressione a causa della manipolazione e della disinformazione, il diritto di accesso a informazioni veritiere e il diritto all'integrità psicologica. Inoltre, le operazioni cognitive mirate rischiano di esacerbare la discriminazione basata su etnia, religione, genere o appartenenza politica, con il rischio di violare il diritto alla non discriminazione.

45. Il rapido sviluppo dell'IA sta trasformando profondamente la diffusione delle informazioni e rendendo la cognizione umana un ambito chiave del confronto militare. Inoltre, simulazioni di realtà virtuale ad alto stress sono impiegate per l'addestramento al combattimento, avvalendosi dei dati raccolti per favorire la preparazione futura. Ciò evidenzia l'alta posta in gioco della competizione nel dominio cognitivo.⁴⁷

F. Potenziale convergenza tra intelligenza artificiale e tecnologie biologiche, comprese le armi biologiche

46. L'IA è divenuta parte integrante delle scienze della vita, favorendo progressi nella biotecnologia atti a coadiuvare la risoluzione di problematiche globali quali la sicurezza alimentare e l'approvvigionamento idrico. Tuttavia, la convergenza tra IA e biotecnologia può comportare gravi rischi per i diritti umani, in particolare attraverso lo sviluppo di armi biologiche potenziate dall'IA. Lo sviluppo, la produzione, l'acquisizione, il trasferimento, lo stoccaggio e l'uso di armi biologiche sono vietati dalla Convenzione sulla proibizione dello sviluppo, della produzione e dello stoccaggio delle armi batteriologiche (biologiche) e a base di tossine e sulla loro distruzione. Tale divieto ha carattere onnicomprensivo, a prescindere dalle tecnologie impiegate, il che implica l'interdizione anche delle armi biologiche potenziate dall'IA.

47. L'integrazione dell'IA con la biologia sintetica, che prevede la riprogettazione di organismi per finalità specifiche, potrebbe agevolare la creazione di organismi interamente nuovi dotati di caratteristiche predefinite. Ciò comporta il rischio di uno sviluppo imprevisto e pericoloso di agenti biologici, con il potenziale insorgere di nuove forme di minacce biologiche.⁴⁸ Inoltre, sebbene l'IA possa facilitare l'accesso alle informazioni e la diffusione della conoscenza, essa può altresì incrementare i rischi di biosicurezza consentendo la condivisione di saperi sensibili con attori fuorviati o malevoli.⁴⁹

48. Le armi biologiche potenziate dall'IA pongono sfide in relazione ai diritti alla vita, all'Integrità, alla salute e a un ambiente pulito, sano e sostenibile. Inoltre, esse potrebbero presentare criticità in termini di biosicurezza e sicurezza biologica sotto il profilo del rilevamento e dell'attribuzione, qualora siano appositamente progettate per eludere i sistemi di monitoraggio esistenti, rendendo complessa l'identificazione e la risposta a un attacco avversario. In aggiunta, le armi biologiche potrebbero essere progettate per simulare focolai naturali, complicando l'attribuzione e gli sforzi volti a individuarne la fonte, precludendo in tal modo una risposta adeguata e ostacolando potenzialmente il diritto a un ricorso effettivo.⁵

49. La gestione di tali rischi richiede un approccio multidimensionale basato sui diritti umani, che includa l'applicazione del diritto internazionale dei diritti umani, il recepimento di quadri internazionali quali la Convenzione sulle armi biologiche, la cooperazione multilaterale, gli investimenti nella biosicurezza e la ricerca sulle tecnologie difensive.

G. Intelligenza artificiale e sistemi di comando e controllo nucleare

50. Sebbene gli Stati dotati di capacità nucleari riconoscano, in una certa misura, i rischi connessi all'integrazione dell'IA nei sistemi di comando e controllo nucleare ai fini della consapevolezza situazionale e del rilevamento delle minacce, il perseguimento di un vantaggio strategico in un contesto nucleare in evoluzione – congiuntamente al timore di accumulare ritardi nell'innovazione dell'IA – potrebbe determinare un'adozione accelerata e prematura di tali sistemi

⁴⁷ Si veda <https://www.act.nato.int/activities/cognitive-warfare/>.

⁴⁸ Anshula Sharma e altri, "Next generation agents (synthetic agents)", in *Handbook on Biological Warfare Preparedness*, S.J.S. Flora e Vidhu Pachaur, a cura di (Londra, Elsevier, 2020).

⁴⁹ Zhaohui Su e altri, "Addressing biodisaster X threats with artificial intelligence and 6G technologies", *Journal of Medical Internet Research*, vol. 23, n. 5 (maggio 2021); e Renan Chaves de Lima et al., "Artificial intelligence challenges in the face of biological threats", *Frontiers in Artificial Intelligence* (maggio 2024).

⁵⁰ Connor O'Brien, Kathleen Varty e Anna Ignaszak, "The electrochemical detection of bioterrorism agents", *Microsystems and Nanoengineering*, vol. 7, n. 1 (2021).

di tali tecnologie.⁵¹ È opportuno distinguere tra l'impiego di sistemi di IA per la consapevolezza situazionale e il rilevamento delle minacce e il suo potenziale utilizzo nei processi decisionali concernenti le armi nucleari. Attualmente, l'impiego dell'IA nei sistemi di comando, controllo e comunicazione nucleare appare incentrato in via prioritaria sul rilevamento precoce delle minacce, sulla raccolta di informazioni e sulle funzioni di supporto alle decisioni. Sebbene sia stata segnalata l'esistenza di un sistema automatico progettato per l'impiego in caso di attacco decapitante, tale sistema è antecedente agli attuali sviluppi dell'IA. L'affidabilità e le implicazioni dell'IA in tali sistemi risultano preoccupanti, segnata-mente qualora i futuri progressi dovessero indurre a un maggiore affidamento su processi decisio-nali guidati dall'IA.⁵²

51. L'integrazione di sistemi di IA avanzati basati sull'apprendimento profondo presenta sfide più ampie rispetto ai modelli vigenti basati su regole predefinite. Le principali criticità includono l'affidabilità, la trasparenza, la vulnerabilità ad attacchi avversari e il disallineamento dei modelli su vasta scala in funzioni critiche, quali i processi decisionali concernenti le armi nucleari.⁵³ I modelli di apprendimento profondo sono intrinsecamente opachi, rendendo i propri processi decisionali difficili da interpretare, il che può de-terminare esiti imprevedibili e compromettere la supervisione umana. Inoltre, la rapidità dei cicli deci-sionali consente all'IA di operare a velocità superiori alle capacità umane, riducendo potenzialmente il tempo disponibile per le decisioni di risposta nucleare a un livello tale da rendere difficoltoso un con-trollo umano efficace. Ciò solleva gravi preoccupazioni in merito alla dignità umana e ai diritti umani, inclusi il diritto alla vita, l'Integrità, la non discriminazione, la salute e il diritto a un ambiente sano.

52. Inoltre, il rischio che i sistemi di IA interpretino erroneamente attività lecite o falsi allarmi come minacce potrebbe causare un'escalation involontaria. Un'ulteriore preoccupazione è costituita dal pregiudizio dell'automazione, per cui gli operatori umani potrebbero fare eccessivo affidamento sulle decisioni assunte dai sistemi di IA, anche qua-lora l'intuizione umana, la consapevolezza derivante dall'addestramento o altre fonti di informazione suggeris-cano una linea d'azione alternativa, con conseguenti potenziali errori di valutazione dagli esiti ad alto rischio. Le attività dolose nel settore delle tecnologie dell'informazione e della comunicazione (TIC) dirette contro i si-stemi di IA potrebbero consentire ad avversari di infiltrarsi, disabilitare, manipolare o contraffare le risposte, determinando incertezza e potenziali errori di valutazione o azioni non intenzionali.⁵⁴ Inoltre, i sistemi di IA si basano necessariamente su ampi set di dati per l'addestramento. Eventuali avversari potrebbero corrompere tali dati, inficiando i processi decisionali e conducendo potenzialmente a violazioni del diritto umano alla non discriminazione.

53. L'integrazione dell'IA nei sistemi di comando e controllo nucleare presenta rischi significativi che devono essere gestiti con cautela attraverso una convergenza di valutazioni dei rischi, salvaguardie tecniche, consi-derazioni etiche e solidi quadri giuridici. Il dinamismo nello sviluppo dell'IA richiede spirito d'iniziativa e un approccio proattivo volto ad accelerare i meccanismi atti a garantire che tali capacità siano im-piegate in modo responsabile, sicuro e in conformità con il diritto internazionale dei diritti umani.

H. Armi a energia diretta

54. Le armi a energia diretta comprendono sistemi che emettono energia concentrata in una direzione specifica senza l'ausilio di proiettili. Nelle applicazioni militari, tali armi si avvalgono di tecnologie elettroma-gnetiche o a particelle, anziché della forza cinetica, per neutralizzare o distruggere gli obiettivi. Tali armi includono laser, microonde, onde millimetriche e fasci di particelle.

Esse possono essere impiegate per scopi non letali, quali l'interferenza o l'abbagliamento di esseri umani, dispo-sitivi e sistemi elettronici.⁵⁵ Qualora utilizzate per fini militari, le armi a energia diretta sono in grado di colpire obiettivi fisici a diversi chilometri di distanza con elevata precisione e accuratezza.

⁵¹ Si veda <https://warontherocks.com/2024/12/beyond-human-in-the-loop-managing-ai-risks-in-nuclear-command-and-control/>.

⁵² Alice Saltini, "IA and nuclear command, control and communications" (Londra, European Leadership Network, 2023).

⁵³ Ibidem.

⁵⁴ Muhammad Mudassar Yamin e altri, "Weaponized AI for cyber-attacks", *Journal of Information Security and Applications*, n. 57 (marzo 2021).

⁵⁵ Bhaman Zohuri, *Directed Energy Weapons* (Svizzera, Springer, 2016).

55. Con il progredire della tecnologia delle armi a energia diretta, i sistemi d'arma divengono sempre più potenti, diffusi e integrati tra le piattaforme aeree, terrestri, marittime e spaziali. La rapidità d'azione alla velocità della luce, la precisione, la scalabilità, l'efficienza logistica e il basso costo per colpo offrono vantaggi sia nelle applicazioni civili che in quelle militari.⁵⁶

56. Nel contesto militare, le armi a energia diretta possono avere ripercussioni sulla popolazione civile. Sebbene sussistano incertezze circa il loro pieno dispiegamento, i recenti prototipi e le applicazioni testimoniano progressi che trascendono lo stadio teorico.⁵⁷ Tali armi possono causare gravi lesioni, incluse cecità e ustioni. Ad esempio, i laser ad alta energia possono causare ustioni ai tessuti, mentre le armi a microonde provocano dolore acuto attraverso il riscaldamento dei liquidi corporei, con il rischio di determinare lesioni gravi e permanenti.⁵⁸ In considerazione di tali effetti, l'impiego di siffatte armi e l'impatto del dispiegamento di energia diretta sollevano serie preoccupazioni in materia di diritti umani, segnatamente per quanto concerne il diritto alla salute, l'integrità fisica, nonché il diritto alla vita e a un ambiente sano. Assume rilevanza il Protocollo addizionale alla Convenzione sulla proibizione o la restrizione dell'uso di alcune armi classiche che possono essere ritenute capaci di causare effetti traumatici eccessivi o di colpire in modo indiscriminato (Protocollo IV, relativo alle armi laser accecanti), il quale proibisce l'uso di armi laser specificamente concepite per causare cecità permanente.

III. Ruolo degli attori statali e non statali nella progettazione, nell'addestramento, nel dispiegamento, nell'impiego e nell'acquisizione di tecnologie nuove ed emergenti nel settore militare

A. Obblighi degli Stati relativi alla prevenzione delle violazioni del diritto internazionale e alla regolamentazione e al monitoraggio delle tecnologie nuove ed emergenti nel settore militare

57. Gli obblighi giuridici internazionali devono essere integrati nelle fasi di progettazione, sviluppo e impiego delle tecnologie nuove ed emergenti nel settore militare. Incombe sugli Stati l'obbligo di garantire che l'applicazione di tali tecnologie sia pienamente conforme al diritto internazionale dei diritti umani, con particolare riferimento ai diritti alla vita, all'integrità fisica, alla non discriminazione, al rispetto della vita privata e a un ambiente sano. Gli obblighi derivanti dal diritto internazionale umanitario rivestono una rilevanza particolare: gli Stati sono tenuti non solo a «rispettare» le norme – introducendo divieti e restrizioni su armi, mezzi e metodi di guerra – ma anche a «far rispettare» il diritto internazionale umanitario. Tuttavia, la definizione di quest'ultimo dovere rimane imprecisa, lasciandone alcuni aspetti soggetti a interpretazione. Inoltre, gli Stati devono procedere a un esame approfondito delle armi.

58. L'obbligo di «far rispettare» impone agli Stati di garantire l'attuazione e l'applicazione del diritto internazionale a livello nazionale; i relativi obblighi di dovuta diligenza si estendono a tutte le misure necessarie per prevenire violazioni da parte di attori pubblici e soggetti privati, inclusi gli sviluppatori di tecnologie nuove ed emergenti. Le due condizioni affinché sorga la responsabilità in caso di dovuta diligenza sono: (a) la disponibilità dei mezzi per prevenire o reprimere la violazione; e (b) l'aver conosciuto o l'aver dovuto conoscere il rischio di violazione.⁵⁹ Tale responsabilità abbraccia l'intero ciclo di vita delle tecnologie nuove ed emergenti, garantendo la conformità con il Diritto internazionale. Inoltre, tale valutazione deve essere effettuata in modo continuativo.

⁵⁶ Cfr. <https://www.nationaldefensemagazine.org/articles/2020/10/13/uptick-in-spending-seen-for-directed-energy-weapons>.

⁵⁷ Cfr. <https://article36.org/wp-content/uploads/2019/06/directed-energy-weapons.pdf>; e <https://nualslawjournal.com/2023/07/25/bringing-directed-energy-weapons-within-the-purview-of-the-arms-control-regime>.

⁵⁸ Gary M. Vilke e Theodore C. Chan, "Less lethal technology", *Policing: An International Journal*, vol. 30, n. 3 (2007); e Erdem Eren Demir e altri, "The role of non-lethal weapons in public security", *Journal of Criminal Law and Criminology*, vol. 60, n. 3 (luglio-dicembre 2022).

⁵⁹ Antal Berkes, "The standard of 'due diligence' as a result of interchange between the law of armed conflict and general international law", *Journal of Conflict and Security Law*, vol. 23, n. 3 (inverno 2018).

59. Gli Stati sono tenuti ad adottare misure atte a prevenire violazioni dei diritti umani nell'ambito della propria giurisdizione.⁶⁰ L'inosservanza di tale obbligo può comportare la responsabilità internazionale. L'impiego di tecnologie nuove ed emergenti nel settore militare impone verosimilmente obblighi supplementari e standard più elevati di dovuta diligenza per garantire l'adozione di tutte le precauzioni fattibili.

60. Uno Stato può altresì essere ritenuto responsabile delle conseguenze della condotta di soggetti privati qualora ometta di adottare le misure necessarie per prevenire, monitorare, regolamentare, investigare o sanzionare tali esiti.⁶¹ Pertanto, gli Stati devono conformarsi agli obblighi di dovuta diligenza nello sviluppo, nell'acquisizione e nell'uso di tecnologie nuove ed emergenti nel settore militare da parte di attori non statali.

61. Il settore privato, in particolare nell'ambito dell'IA, può sviluppare tecnologie suscettibili di applicazioni nel settore militare. L'urgenza della commercializzazione induce sovente a sottostimare i rischi, tra cui l'uso improprio dell'IA generativa in operazioni TIC malevole o in campagne di disinformazione. Un'ulteriore criticità risiede nella proliferazione incontrollata di tali tecnologie, che ne consente l'acquisizione da parte di attori non statali. Tali attori impiegano frequentemente tecnologie nuove ed emergenti nel settore militare in assenza di adeguate salvaguardie e con minori requisiti di accuratezza o affidabilità rispetto agli attori statali. Gli attori non statali potrebbero altresì avvalersi di tecnologie nuove ed emergenti per perturbare o alterare i sistemi di comunicazione, compromettendone l'accuratezza e l'affidabilità.

62. La rapida espansione dell'IA e dei dispositivi connessi all'Internet degli oggetti⁶² è destinata a rivestire un ruolo determinante nelle future operazioni cibernetiche in ambito militare. Lo sfruttamento di tali tecnologie potrebbe introdurre o aggravare le vulnerabilità, permettendo ad attori non statali di manipolare l'IA, compromettere i sistemi dell'Internet degli oggetti, interrompere servizi essenziali, quali l'assistenza sanitaria, o perpetrare reati informatici. Tali attacchi possono causare violazioni di dati, fallimenti operativi, danni fisici e minacce alla vita e all'integrità.⁶³

63. Considerati i molteplici rischi connessi all'acquisizione o allo sviluppo di tecnologie nuove ed emergenti nel settore militare da parte di attori non statali, gli Stati sono gravati da un obbligo giuridico internazionale di dovuta diligenza volto a indagare efficacemente e a istituire rimedi effettivi per le violazioni dei diritti umani, nonché a sanzionare i soggetti responsabili di tali violazioni. Ciò richiede l'adozione di misure quali un solido quadro normativo a tutela dei diritti alla vita, dell'integrità, della non discriminazione, della salute, di un ambiente sano e del rispetto della vita privata; un monitoraggio rafforzato, che includa il potenziamento della cybersicurezza; la cooperazione internazionale; e una formazione esaustiva per le parti interessate in merito ai rischi potenziali e all'uso improprio delle tecnologie nuove ed emergenti nel settore militare. Il mancato contrasto di tali rischi potrebbe determinare violazioni dei diritti alla vita, dell'integrità, del rispetto della vita privata e della non discriminazione.

B. Fornitori e imprese di tecnologie nuove ed emergenti nel settore militare

64. Gli Stati rappresentano i principali utilizzatori di tecnologie nuove ed emergenti nell'ambito della difesa nazionale e della sicurezza pubblica. Essi promuovono altresì lo sviluppo di tali tecnologie attraverso il finanziamento della ricerca e la promozione di partenariati pubblico-privati. Le entità private, inclusi i contraenti nel settore della difesa e le imprese operanti nel campo delle TIC, agiscono in qualità di innovatori e sviluppatori, fornendo servizi quali lo sviluppo, l'implementazione, la manutenzione e la formazione.

65. A livello nazionale, gli Stati operano in qualità di regolatori delle tecnologie nuove ed emergenti attraverso la definizione di quadri giuridici e standard per le imprese, le quali sono tenute a conformarsi agli obblighi statali sanciti dal diritto internazionale dei diritti umani. Tale ordinamento impone agli Stati l'obbligo vincolante di rispettare, proteggere e attuare i diritti umani con riferimento alle tecnologie nuove ed emergenti nel settore militare. Inoltre, le imprese interessate devono conformarsi alla normativa vigente e rispettare i diritti umani, secondo quanto delineato nei Principi guida. Tale responsabilità si applica a tutte

⁶⁰ Vedere [A/HRC/30/20](#).

⁶¹ Articoli sulla responsabilità degli Stati per atti internazionalmente illeciti.

⁶² L'Internet degli oggetti consiste in una rete di dispositivi interconnessi atti alla condivisione di dati in tempo reale. Nel settore militare, esso mette in rete sensori, veicoli ed equipaggiamenti al fine di potenziare la sorveglianza, la logistica e i processi decisionali.

⁶³ Nicholas Tsagourias, "Cyber attacks, self-defence and the problem of attribution", *Journal of Conflict and Security Law*, vol. 17, n. 2 (2012).

imprese, comprese le società tecnologiche, a prescindere dalle dimensioni o dalla struttura. ⁶⁴ Le imprese hanno l'obbligo di prevenire violazioni dei diritti umani e di rimediare a eventuali impatti negativi. Qualora si verificano violazioni, gli Stati hanno il dovere di indagare e devono garantire che le vittime abbiano accesso a ricorsi effettivi, anche attraverso adeguati strumenti giudiziari o extragiudiziari. I Principi guida e il Gruppo di lavoro sulla questione dei diritti umani e delle società transnazionali e altre imprese costituiscono elementi chiave per la prevenzione e la mitigazione delle violazioni. In tal senso, il Gruppo di lavoro ha rilevato che le imprese del settore degli armamenti spesso omettono di applicare un'adeguata diligenza dovuta in materia di diritti umani, segnatamente nella valutazione dei rischi connessi all'impiego dei propri dispositivi in situazioni di conflitto. ⁶⁵ Inoltre, il Progetto B-Tech dell'Ufficio dell'Alto Commissariato delle Nazioni Unite per i Diritti Umani fornisce orientamenti autorevoli e risorse per l'attuazione dei Principi guida nell'ambito tecnologico e sollecita le imprese e i decisori politici ad adottare un approccio basato sui diritti umani per affrontare le sfide derivanti dalle nuove tecnologie. ⁶⁶

IV. Diritti umani nel ciclo di vita delle tecnologie nuove ed emergenti nel settore militare

A. Prospettiva basata sul ciclo di vita

66. Le tecnologie nuove ed emergenti nel settore militare presentano sfide uniche per la tutela e la promozione dei diritti umani. Molte di tali tecnologie hanno una natura a duplice uso, il che rende più complessa la situazione relativa alla ripartizione delle responsabilità tra Stati e soggetti privati. Un solido approccio basato sul ciclo di vita è essenziale per affrontare efficacemente tali sfide, garantendo la salvaguardia dei diritti umani dalle fasi di sviluppo e addestramento fino alla distribuzione, all'impiego operativo e all'eventuale smaltimento o dismissione.

1. Integrazione dei diritti umani nelle fasi di progettazione e sviluppo

67. La fase di concettualizzazione e di progettazione delle tecnologie nuove ed emergenti nel settore militare è cruciale per integrare le considerazioni relative ai diritti umani sin dall'inizio. Essa comprende l'ideazione iniziale e lo sviluppo della tecnologia, ambito in cui le potenziali ripercussioni sui diritti umani dovrebbero essere rigorosamente valutate. Le tecnologie non sono neutrali; esse influenzano intrinsecamente la definizione delle politiche e possono limitare le libertà individuali. ⁶⁷ In quanto tali, sia la tecnologia stessa sia i suoi creatori possono incidere sui diritti umani, in quanto riflettono spesso valori e distorsioni specifici. ⁶⁸ L

'esecuzione di valutazioni d'impatto sui diritti umani in tali fasi precoci risulta fondamentale.

Tali valutazioni dovrebbero essere integrate nel processo di sviluppo al fine di identificare e mitigare i rischi potenziali per i diritti umani, inclusi i diritti al rispetto della vita privata, alla libertà di espressione, alla vita, all'integrità, alla salute e a un ambiente sano. Sebbene l'integrazione di tali considerazioni nella fase di progettazione possa coadiuvare gli sviluppatori nel minimizzare le conseguenze indesiderate e gli usi impropri, essa potrebbe non risolvere appieno le tensioni giuridiche intrinseche derivanti da determinate tecnologie. Permangono dubbi circa la piena compatibilità con gli standard dei diritti umani di tecnologie quali quelle impiegate nei sistemi di armi autonome, in particolare qualora il loro utilizzo pregiudichi principi fondamentali quali la tutela della dignità umana. Pertanto, la garanzia di conformità agli standard internazionali sui diritti umani può, in taluni casi, richiedere quadri normativi di più ampio respiro atti a disciplinare le peculiari questioni giuridiche sollevate da tali tecnologie.

69. Lo sviluppo di tecnologie nuove ed emergenti nel settore militare comporta sovente l'impiego di vasti set di dati, suscettibili di incorporare e perpetuare distorsioni. Onde prevenire la discriminazione, è essenziale implementare, durante la fase di progettazione, algoritmi basati sui diritti umani e attenti ai criteri di equità, nonché analisi controfattuali. Si raccomanda agli sviluppatori di tenere in considerazione la diversità all'interno

⁶⁴ Si veda <https://www.ohchr.org/sites/default/files/2021-11/tech-2021-response-export-military-software.pdf>.

⁶⁵ Si veda <https://www.ohchr.org/sites/default/files/2022-08/BHR-Arms-sector-info-note.pdf>.

⁶⁶ Si veda <https://untoday.org/un-b-tech-project/>.

⁶⁷ A/HRC/47/52, par. 4.

⁶⁸ Andrew Feenberg, *Transforming Technology* (Oxford, Oxford University Press, 2002); e Cathy O'Neil, *Weapons of Math Destruction* (New York, Crown, 2016).

dei propri gruppi di sviluppo e di espletare verifiche sulla diversità al fine di ridurre la probabilità di utilizzare set di dati e programmazioni distorti che possano alimentare i pregiudizi

70. Le imprese coinvolte nello sviluppo di tecnologie nuove ed emergenti hanno il dovere di conformare le proprie attività al diritto internazionale dei diritti umani, con particolare riferimento ai Principi guida. Ciò implica l'esercizio della dovuta diligenza per garantire che tali tecnologie non concorrano a violazioni dei diritti umani, sia in ambito militare che civile. In virtù del dovere di dovuta diligenza in capo agli Stati, questi ultimi sono tenuti a regolamentare gli ambiti in cui operano i soggetti privati e a stabilire obblighi a livello nazionale affinché le imprese si conformino ai diritti umani.

2. Gestione dei rischi durante le fasi di schieramento e di impiego operativo

71. Con il passaggio delle tecnologie nuove ed emergenti alla fase di impiego operativo, il rischio di violazioni dei diritti umani tende a intensificarsi. Risulta fondamentale stabilire standard giuridici rigorosi che garantiscano la dignità umana, un controllo umano significativo, la trasparenza e l'obbligo di rendere conto in ogni fase di schieramento e impiego, segnatamente negli scenari in cui l'automazione e l'IA possano comportare la perdita di un controllo umano significativo, distorsioni da automazione o l'uso improprio della tecnologia in violazione del diritto internazionale.

72. I processi di verifica, sperimentazione e valutazione dovrebbero coinvolgere gruppi eterogenei al fine di correggere potenziali distorsioni, tenendo conto di fattori quali l'età, l'origine etnica e il genere. Ciò contribuisce a garantire che le tecnologie nuove ed emergenti nel settore militare non aggravino ulteriormente le ripercussioni negative sui diritti umani a danno delle popolazioni vulnerabili, né perpetuino le disuguaglianze esistenti. Gli Stati dovrebbero adottare un quadro normativo basato sul rischio, applicando regolamentazioni più stringenti o divieti per le tecnologie ad alto rischio che rappresentano minacce significative per la vita, la salute, la sicurezza personale e altri diritti umani.

73. La trasparenza risulta fondamentale nell'impiego delle tecnologie nuove ed emergenti, segnatamente con riferimento ai dati e agli algoritmi utilizzati. Occorre avvalersi di tecniche di dovuta diligenza, quali strumenti di rilevamento delle distorsioni o verifiche algoritmiche, al fine di identificare e correggere le distorsioni nei risultati prodotti dai sistemi.

3. Misure di salvaguardia durante lo smaltimento, la dismissione e la prevenzione della proliferazione

74. La fase finale del ciclo di vita delle tecnologie nuove ed emergenti nel settore militare – lo smaltimento o la dismissione – presenta specifiche implicazioni in materia di sicurezza e di diritti umani. Tale fase comporta lo smantellamento fisico delle tecnologie, lo smaltimento sicuro dei materiali pericolosi e la protezione di ogni dato sensibile raccolto durante il periodo operativo. L'attuazione di misure di salvaguardia volte a prevenire lo storno di materiali dalle scorte e la vendita non autorizzata di equipaggiamenti eccedentari è essenziale per contrastare i rischi di proliferazione. Assicurare che tali processi siano gestiti con trasparenza e nel rispetto dell'obbligo di rendere conto, prevenendo impatti differenziati sulle popolazioni storicamente emarginate, quali i popoli indigeni e le donne, è imprescindibile per la tutela dei diritti umani.⁶⁹

75. Alla luce della rapida evoluzione delle tecnologie nuove ed emergenti nel settore militare, è imperativo adottare misure proattive e globali per la salvaguardia dei diritti umani. La suddetta analisi sottolinea la necessità di rafforzare il quadro giuridico internazionale, di accrescere l'obbligo di rendere conto da parte delle imprese e di consolidare la cooperazione multilaterale. Istituito rigorosi meccanismi di monitoraggio e promuovendo la trasparenza e la responsabilità legale, la comunità internazionale può garantire che lo sviluppo, l'impiego e la dismissione di tecnologie nuove ed emergenti nel settore militare avvengano nel rispetto dei principi dei diritti umani.

⁶⁹ Si veda [A/75/290](#).

B. Trasparenza e obbligo di rendere conto

76. La proliferazione di tecnologie nuove ed emergenti pone sfide giuridiche e normative senza precedenti. L'IA solleva interrogativi circa l'adeguatezza dei quadri normativi vigenti.⁷⁰ Qualora sussistano rischi elevati per i diritti umani, aumenta la pressione per accelerare la revisione di tali quadri e per istituire nuovi meccanismi di trasparenza e di obbligo di rendere conto.⁷¹

77. Le tecnologie nuove ed emergenti possono potenziare l'esecuzione di compiti complessi, agendo quali moltiplicatori di forza in grado di migliorare la rapidità, la precisione e le capacità umane.⁷² Esse trovano un impiego crescente nelle attività di intelligence, sorveglianza e ricognizione, nel processo decisionale in ambito militare e in funzioni quali la verifica e la selezione degli obiettivi.⁷³ Tuttavia, tali sistemi si configurano spesso come "scatole nere", di difficile interpretazione e ancor più complessi da spiegare. Data l'importanza della prevedibilità e della comprensibilità nell'ambito dell'IA, risulta fondamentale garantire che tali sistemi operino come previsto e in modo intelligibile. Gli sforzi volti a chiarire il funzionamento interno delle tecnologie si stanno dimostrando sempre più innovativi, producendo risultati significativi nel promuovere la trasparenza. Le attività di ricerca per l'avanzamento dell'intelligenza artificiale spiegabile sono cresciute considerevolmente, conseguendo successi nel rendere l'IA più trasparente e facilitandone potenzialmente l'adozione in settori critici ad alto rischio.⁷⁴ Il valore intrinseco dello sviluppo di un'intelligenza artificiale spiegabile risiede nel rispondere alle preoccupazioni relative alla carenza di trasparenza e dell'obbligo di rendere conto. Tuttavia, i rischi associati all'implementazione dell'intelligenza artificiale spiegabile, quali le violazioni del rispetto della vita privata e le vulnerabilità dei sistemi derivanti da una maggiore trasparenza, non devono essere sottovalutati.

78. Il diritto internazionale dei diritti umani impone il rispetto del principio di trasparenza. Nel contesto delle tecnologie nuove ed emergenti nel settore militare, ciò implica garantire l'accesso alle informazioni pertinenti relative al loro sviluppo, impiego e impatto. La trasparenza è altresì essenziale per conformarne l'utilizzo al diritto internazionale, salvaguardando i diritti alla libertà di opinione e di espressione, al rispetto della vita privata, alla non discriminazione e all'uguaglianza.

79. Inoltre, una questione rilevante nell'affrontare i rischi legati alle tecnologie nuove ed emergenti nel settore militare concerne la misura in cui le capacità decisionali integrate nei sistemi possano riflettere le distorsioni esistenti e le forme di discriminazione prevalenti nella società. Una delle sfide principali consiste nel garantire che le lacune di rappresentatività nella raccolta dati, nel trattamento e nella conservazione degli stessi non perpetuino o esacerbino le violazioni dei diritti umani. L'affrontare tali questioni richiede trasparenza e rigorose misure in materia di obbligo di rendere conto, volte a ritenere tutti gli attori responsabili dell'uso etico e lecito delle tecnologie nuove ed emergenti.

C. Lacune nell'attuale quadro normativo in materia di diritti umani

80. Le tecnologie nuove ed emergenti nel settore militare pongono sfide all'applicazione dei quadri normativi vigenti in materia di diritti umani. Sebbene la conformità al diritto internazionale sia essenziale, occorre colmare lacune critiche per garantire la protezione dei diritti umani in tale contesto. Nonostante l'importanza dei Principi guida e dell'operato del progetto B-Tech dell'OHCHR, si rileva l'assenza di standard internazionali sui diritti umani che specifichino, nel contesto delle tecnologie nuove ed emergenti nel settore militare, gli obblighi che il diritto internazionale dei diritti umani vigente impone sia agli Stati che agli attori non statali. Inoltre, a livello nazionale, le nuove tecnologie e

⁷⁰ Stefan Larsson e Fredrik Heintz, "Trasparenza nell'intelligenza artificiale", *Internet Policy Review*, vol. 9, n. 2 (2020); e Jordan Richard Schoenherr e altri, "Progettare l'IA secondo un approccio incentrato sull'essere umano", *IEEE Transactions on Technology and Society*, vol. 4, n. 1 (marzo 2023).

⁷¹ Cfr. A/HRC/48/31.

⁷² Jonathan Han Chung Kwik e Tom van Engers, "Nebbia di guerra algoritmica", *Journal of Future Robot Life*, vol. 2, n. 1 (2021).

⁷³ Hannah Bryce e Jacob Parakilas, "Conclusioni e raccomandazioni", in *Artificial Intelligence and International Affairs: Disruption Anticipated*, M.L. Cummings e altri, a cura di (Londra, Chatham House, 2018); e Comitato Internazionale della Croce Rossa, "Intelligenza artificiale e apprendimento automatico nei conflitti armati: un approccio incentrato sull'essere umano" (Ginevra, 2019).

⁷⁴ Arthur Holland Michel, "The black box, unlocked" (Istituto delle Nazioni Unite per la ricerca sul disarmo, 2020); e Arun Das e Paul Rad, "Opportunities and challenges in explainable artificial intelligence (XAI)", *arXiv preprint* (2020).

⁷⁵ Si veda https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2023-11-16-techdispatch-22023-explainable-artificial-intelligence_en.

le tecnologie emergenti nel settore militare rimangono ampiamente deregolate, data la carenza di quadri legislativi o programmatici volti a guidare l'industria e gli sviluppatori nella progettazione, nello sviluppo e nella sperimentazione di tecnologie nuove ed emergenti nel settore militare, al fine di garantire l'istituzione di chiari perimetri di protezione in conformità con gli obblighi giuridici internazionali.

81. Risultano carenti, ad esempio, strategie di approvvigionamento trasparenti che abbraccino l'intera catena di fornitura delle tecnologie nuove ed emergenti nel settore militare e che definiscano garanzie basate sul diritto internazionale dei diritti umani, determinando così il rischio di impieghi discriminatori di talune tecnologie. Inoltre, l'assenza di meccanismi di supervisione internazionale per lo sviluppo, l'approvvigionamento e l'impiego di tali tecnologie nel settore militare ostacola l'attuazione efficace degli obblighi giuridici internazionali, segnatamente nei casi in cui le normative nazionali si dimostrino insufficienti. Sebbene alcuni Stati abbiano adottato quadri normativi, permangono lacune significative nelle procedure nazionali di controllo e verifica basate sui Principi guida per le imprese e i fornitori di tecnologie nuove ed emergenti del settore privato, il che limita la capacità di garantire la conformità agli standard del diritto internazionale dei diritti umani. Affrontare tali lacune normative è fondamentale per prevenire violazioni e abusi dei diritti umani derivanti dallo sviluppo e dall'impiego di tecnologie nuove ed emergenti nel settore militare.

82. Un'ulteriore lacuna critica nell'attuale quadro normativo in materia di diritti umani concerne l'impatto ambientale delle tecnologie nuove ed emergenti. Le fasi di sviluppo, addestramento e dispiegamento di tali tecnologie comportano un elevato consumo energetico, un'impronta di carbonio rilevante e l'uso intensivo di materie prime quali nichel, cobalto e grafite, determinando conseguenze ambientali a lungo termine.⁷⁶ Queste includono il raffreddamento dei centri dati, che richiede un ingente consumo idrico, e lo smaltimento di rifiuti pericolosi in fase di smantellamento. La tutela dei diritti ambientali resta problematica a causa della carenza di quadri giuridici globali e di meccanismi sanzionatori. La trasparenza nella divulgazione delle informazioni, un monitoraggio ambientale rigoroso e un quadro collaborativo in materia di obbligo di rendere conto sono elementi essenziali per la salvaguardia del diritto umano a un ambiente sano.

V. Raccomandazioni

A. Stati e comunità internazionale

83. Gli Stati dovrebbero elaborare con urgenza strategie e politiche nazionali e regolamentare la progettazione, lo sviluppo e l'uso responsabili delle tecnologie nuove ed emergenti nel settore militare, in conformità con i propri obblighi ai sensi del diritto internazionale. Ciò comporta la creazione di solidi quadri di revisione delle armi che affrontino le sfide peculiari poste dalle armi basate su tecnologie nuove ed emergenti e l'istituzione di meccanismi preventivi e di accertamento della responsabilità efficaci per il loro sviluppo e impiego.

Inoltre, i meccanismi istituzionali dovrebbero essere rafforzati al fine di anticipare e affrontare potenziali violazioni dei diritti umani, con particolare attenzione al potenziamento delle capacità di controllo degli enti locali, quali le istituzioni nazionali per i diritti umani.

84. Gli Stati e le organizzazioni internazionali dovrebbero integrare le considerazioni relative al diritto internazionale dei diritti umani in tutti i negoziati multilaterali sulle tecnologie nuove ed emergenti nel settore militare, segnatamente nel Gruppo di lavoro II della Commissione per il disarmo, in merito alle sue raccomandazioni sulle intese comuni relative alle tecnologie emergenti nella sicurezza internazionale. Ogni quadro di riferimento sviluppato deve affrontare i rischi per i diritti umani, incluse le pratiche discriminatorie, congiuntamente alle preoccupazioni in materia di sicurezza. Inoltre, il quadro del diritto internazionale dei diritti umani deve essere incluso nelle discussioni sui sistemi di armi autonome, segnatamente in seno al Gruppo di esperti governativi.

85. Gli Stati dovrebbero perseguire partenariati strategici volti ad affrontare le sfide rilevanti in materia di sicurezza. Il proseguimento del dialogo, lo scambio di migliori pratiche e la definizione di quadri inclusivi che coinvolgano gli Stati, il settore privato, il mondo accademico e altre parti interessate contribuiranno a garantire

⁷⁶ Wichuta Teeratanabodee, "The environmental impact of military AI", IDSS Paper No. 039 (S. Rajaratnam School of International Studies, 2022).

la stabilità e la mitigazione dei rischi. Si dovrebbe altresì attribuire priorità alla condivisione degli esami di legittimità giuridica relativi alle tecnologie nuove ed emergenti nel settore militare. Inoltre, il rafforzamento della collaborazione tra le comunità scientifiche e tecniche, la società civile e i difensori e professionisti dei diritti umani promuoverà l'uso responsabile delle tecnologie nuove ed emergenti nel settore militare.

86. Gli Stati e le organizzazioni internazionali dovrebbero considerare l'adozione di misure vincolanti o di altre misure efficaci atte a garantire che le tecnologie nuove ed emergenti nel settore militare, la cui progettazione, sviluppo o impiego comporti rischi significativi di uso improprio, abuso o danno irreversibile – in particolare qualora tali rischi possano sfociare in violazioni dei diritti umani – non siano sviluppate, dispiegate o utilizzate. Ciò include le tecnologie di sorveglianza di massa che violano il rispetto della vita privata, nonché le biotecnologie e le neurotecnologie che minacciano l'integrità fisica e mentale, specialmente in contesti coercitivi.

87. Gli Stati dovrebbero garantire categoricamente che i sistemi di armi autonome non siano sviluppati o dispiegati a meno che non operino sotto un controllo umano significativo. Devono essere adottate normative chiare e vincolanti per garantire la piena conformità con le norme giuridiche internazionali.

88. Gli Stati dovrebbero applicare la dovuta diligenza e il principio di precauzione, conducendo valutazioni dei rischi e valutazioni d'impatto sui diritti umani su tutte le tipologie di tecnologie nuove ed emergenti nel settore militare. Organismi indipendenti, quali le istituzioni nazionali per i diritti umani, dovrebbero guidare tali valutazioni al fine di garantire la partecipazione pubblica e il controllo democratico. Gli esiti di tali valutazioni dovrebbero orientare gli Stati nell'adozione di misure atte a prevenire danni, sospendere le tecnologie ad alto rischio e imporre norme per l'uso militare responsabile delle tecnologie nuove ed emergenti nel settore militare. La collaborazione con i quadri internazionali esistenti – quali quelli previsti dalla Convenzione sulla proibizione dello sviluppo, produzione, stoccaggio e uso di armi chimiche e sulla loro distruzione e dalla Convenzione sulle armi biologiche, che proibiscono lo sviluppo, la produzione, l'acquisizione, lo stoccaggio, il trasferimento o l'uso di armi biologiche, tossiniche e chimiche – risulta essenziale per rafforzare la governance e la risposta globale alle tecnologie nuove ed emergenti.

89. Gli Stati e le organizzazioni internazionali dovrebbero adottare un approccio collaborativo alla governance delle tecnologie nuove ed emergenti nel settore militare, garantendo la conformità al diritto internazionale e affrontando al contempo gli impatti sproporzionati sulle nazioni con minori risorse, poiché le disparità nell'IA e nella tecnologia militare non solo esacerbano le disuguaglianze esistenti, ma rischiano altresì di alimentare l'instabilità a lungo termine. Gli Stati che dispongono delle capacità necessarie – segnatamente gli Stati sviluppatori – dovrebbero mitigare i danni attraverso la condivisione delle conoscenze, la fornitura di assistenza tecnica e il contrasto agli effetti destabilizzanti.

B. Imprese

90. Le imprese, in particolare nei settori della difesa e della sicurezza, sono tenute a rispettare i diritti umani in conformità ai Principi guida, istituendo misure di salvaguardia misurabili e adatte ai contesti specifici, al fine di eliminare pregiudizi e discriminazione attraverso valutazioni d'impatto sui diritti umani. Tali misure dovrebbero, nella misura del possibile, tenere conto del segreto industriale, includendo la rendicontazione aziendale e la verifica indipendente, per garantire una partecipazione civica inclusiva e diversificata. Inoltre, le società devono conformarsi alle normative statali, sviluppando e adottando ulteriormente standard basati sul rischio per i diritti umani che includano requisiti di trasparenza, con meccanismi periodicamente riesaminati per garantirne l'efficacia e l'allineamento al diritto internazionale dei diritti umani.

91. Le imprese sono tenute ad adottare e attuare un processo di diligenza dovuta in materia di diritti umani volto a identificare, prevenire, mitigare e rendere conto degli effetti delle tecnologie nuove ed emergenti nel settore militare sui diritti umani, in conformità con i Principi guida. Esse devono inoltre valutare proattivamente i rischi associati a tali tecnologie e modelli di IA, compresi gli impatti sui diritti umani e sulla sicurezza internazionale. Qualora i test relativi a rischi estremi siano soggetti a vincoli di segretezza per motivi di difesa, il coordinamento con le autorità nazionali prima della diffusione è essenziale per garantire la conformità al diritto internazionale.

C. Tutte le parti interessate

92. Tutte le parti interessate, compresi il mondo accademico, le imprese, la società civile, le organizzazioni internazionali e gli Stati, dovrebbero privilegiare la ricerca relativa alle implicazioni per i diritti umani delle tecnologie nuove ed emergenti nel settore militare, sostenendo politiche di valutazione degli impatti delle tecnologie dirompenti e riaffermando l'interdipendenza, l'indivisibilità e l'universalità di tutti i diritti umani in ogni fase del processo di sviluppo.

93. Tutte le parti interessate devono cooperare per garantire lo sviluppo e l'impiego responsabili delle tecnologie nuove ed emergenti nel settore militare, assicurando che la regolamentazione di tali tecnologie resti allineata ai progressi tecnologici e promuovendo il dialogo internazionale per l'elaborazione e l'attuazione di quadri giuridici a tutela dei diritti umani

.

Documento tradotto in italiano dal team di M-Power Translations.

Canale Telegram:

<https://t.me/mpowertranslations>