€ ??,00

ISBN/EAN
9 791221 119312

40

A. Gattini (*a cura di*) – LA TECNO-SOVRANITÀ NELLA PROSPETTIVA DEL DIRITTO INTERNAZIONALE

QUADERNI DEL DIPARTIMENTO DI DIRITTO PUBBLICO INTERNAZIONALE E COMUNITARIO
Nuova serie
Università degli Studi di Padova

LA TECNO-SOVRANITÀ NELLA PROSPETTIVA DEL DIRITTO INTERNAZIONALE

a cura di

Andrea Gattini

G. Giappichelli Editore

QUADERNI DEL DIPARTIMENTO DI DIRITTO PUBBLICO INTERNAZIONALE E COMUNITARIO
Nuova serie
Università degli Studi di Padova

40

LA TECNO-SOVRANITÀ NELLA PROSPETTIVA DEL DIRITTO INTERNAZIONALE

a cura di

Andrea Gattini

G. Giappichelli Editore

VIA PO 21 - TEL.: 011-81.53.111

http://www.giappichelli.it

ISBN/EAN 979-12-211-1931-2
ISBN/EAN 979-12-211-8412-9 (ebook - pdf)
ISBN/EAN 979-12-211-8413-6 (ebook - epub)

Il volume è pubblicato con il contributo finanziario del Dipartimento di Diritto Pubblico, Internazionale e Comunitario dell'Università di Padova - Unione Europea - Next Generation EU, Missione 4 Componente 1, "Social Cohesion and International Law" (SCIL) - CUP C53D23002940006 – responsabile dell'unità operativa prof. Andrea Gattini.

Stampa: Rotolito S.p.A. - Pioltello (MI)

INDICE

pag.

LE MINACCE IBRIDE ALLA PROVA DEL DIRITTO INTERNAZIONALE

REBEKKA MONICO

EU TECH REGULATION AND DIGITAL SOVEREIGNTY

ANTONIO SEGURA-SERRANO

LE NORME TECNICHE INTERNAZIONALI TRA TENSIONI E MISURE A TUTELA DELLA SOVRANITÀ DIGITALE EUROPEA

ANNALISA VOLPATO

pag.

IL GDPR NEL QUADRO DELLE INIZIATIVE EUROPEE PER LA SOVRANITÀ DIGITALE ALL'INDOMANI DEL REGOLAMENTO SULL'INTELLIGENZA ARTIFICIALE

CHIARA CELLERINO

SFIDE E OPPORTUNITÀ NEL RECEPIMENTO DELLA DIRETTIVA DELL'UE SULLE MISURE PER UN LIVELLO COMUNE ELEVATO DI CIBERSICUREZZA (NIS2)

FRANCESCO PAOLO MICOZZI

pag.

PARTE SECONDA

SOVRANITÀ TECNOLOGICA E DIRITTI INDIVIDUALI

pag.

IL DIRITTO D'AUTORE ALLA PROVA DELL'INTELLIGENZA ARTIFICIALE GENERATIVA: CRITICITÀ E SOLUZIONI NELLA PROSPETTIVA DEL DIRITTO INTERNAZIONALE

CARLOTTA CERETELLI

MECCANISMI DI *SCREENING* DEGLI INVESTIMENTI ESTERI FRA SOVRANITÀ TECNOLOGICA E DIRITTO INTERNAZIONALE

MARCO DIMETTO

pag.

AUTORI

Pia ACCONCI, Professoressa ordinaria di Diritto internazionale presso l'Università degli Studi di Teramo.

Antonio BALSAMO, Presidente della Corte d'Appello di Palermo.

Carlotta CERETELLI, Ricercatrice di Diritto internazionale presso l'Università degli Studi di Padova.

Chiara CELLERINO, Professoressa associata di Diritto dell'Unione Europea presso l'Università degli Studi di Genova.

Marco DIMETTO, Ricercatore di Diritto internazionale presso l'Università degli Studi di Padova.

Andrea GATTINI, Professore ordinario di Diritto internazionale presso l'Università degli Studi di Padova.

Riccardo LEONCINI, Professore ordinario di Economia Politica presso l'Alma Mater Studiorum – Università di Bologna.

Francesco Paolo MICOZZI, Dottore di Ricerca, già Professore a contratto presso l'Università degli Studi di Perugia.

Gustavo MINERVINI, Ricercatore di Diritto internazionale presso l'Università degli Studi di Torino.

Rebekka MONICO, Ricercatrice di Diritto internazionale presso l'Università degli Studi dell'Insubria.

Anna Maria PICOZZI, Sostituto procuratore generale presso la Corte d'Appello di Palermo.

Matteo SARZO, Professore associato di Diritto internazionale presso l'Università degli Studi di Padova.

Antonio SEGURA-SERRANO, Professore ordinario presso l'Università di Granada.

Sara TONOLO, Professoressa ordinaria di Diritto internazionale presso l'Università degli Studi di Padova.

Annalisa VOLPATO, Professoressa associata di Diritto dell'Unione Europea presso l'Università degli Studi di Padova.

Parte Prima
IL RUOLO DELLE ORGANIZZAZIONI INTERNAZIONALI

LA RICERCA DEL DIRITTO INTERNAZIONALE IN TEMA DI SICUREZZA DIGITALE NELLA PROSPETTIVA DELLE ORGANIZZAZIONI INTERNAZIONALI

PIA ACCONCI [1]

SOMMARIO: 1. Considerazioni introduttive. – 2. Sicurezza digitale attraverso l'attività delle organizzazioni internazionali. – 3. La sicurezza digitale strumentale al mantenimento della pace e sicurezza internazionale, allo sviluppo sostenibile, alla tutela dei diritti della persona, all'attendibilità dell'informazione, alla stabilità dell'economia di mercato e del commercio internazionale, al tempo della diffusione dell'intelligenza artificiale. – 4. Le organizzazioni internazionali regionali di fronte alla diffusione della tecnologia digitale, in particolare dell'intelligenza artificiale. – 5. Considerazioni conclusive.

1. *Considerazioni introduttive*

Merita svolgere anzitutto alcune considerazioni d'insieme relativamente alla sicurezza digitale (*cybersecurity*).

Gli sviluppi del processo di digitalizzazione possono generare vulnerabilità e complessità e, in maniera ricorrente, alcuni problemi di sicurezza nella realtà dei rapporti internazionali, quali :prevenzione e gestione dell'impiego di tecnologie sofisticate per l'uso e/o la minaccia della forza; usi della tecnologia e *software* suscettibili di esporre le persone, vuoi fisiche vuoi giuridiche a *traffic interception*, *phishing attacks*, furti di *password* e d'identità, perdite finanziarie e/o reputazionali; attacchi

[1] Questo scritto è il risultato di attività di studio e ricerca realizzate dall'a. grazie anche all'associazione con incarico di collaborazione all'Istituto del CNR di Studi giuridici internazionali per il progetto su "Gli ordinamenti giuridici alla prova dei cambiamenti tecnologici e climatici" e al coordinamento del Modulo *Jean Monnet* su "EU against Disinformation through Investment in Information and Communication (EUAD)", Progetto numero 101177052, finanziato dall'Unione europea. Le opinioni espresse appartengono, tuttavia, al solo autore e non riflettono necessariamente le opinioni dell'Unione europea o dell'Agenzia esecutiva europea per l'istruzione e la cultura (EACEA). Né l'Unione europea né l'EACEA possono esserne ritenute responsabili.

alle infrastrutture e alla gestione dei dati di enti pubblici in grado di generare instabilità sociopolitica e militare; conseguente necessità di attività di recupero dei dati e ripristino della situazione precedente; salvaguardia dell'integrità e riservatezza delle informazioni; dinamiche del commercio internazionale.

La natura in continuo cambiamento dei rischi altera sia l'allineamento tra diritto e realtà sia l'aggiornamento delle pratiche di sicurezza. L'intersezione tra tecnologie informatiche e *software* fondati sull'intelligenza artificiale, da alcuni definita la "quarta rivoluzione industriale", ha reso l'ambito di riferimento e il rapporto tra innovazione tecnologica e sicurezza più complessi [2]. La circolazione di prodotti fondati sull'intelligenza artificiale può favorire, infatti, il potenziamento della sicurezza [3] oppure la sofisticazione delle minacce e dei rischi per la sicurezza digitale, alterando quelli esistenti [4].

---

[2] Per intelligenza artificiale si intende comunemente il modo in cui i processi mentali individuali più complessi possono essere riprodotti mediante l'uso di un computer e di simulazioni informatiche. I dati e le informazioni sono acquisiti dall'esterno e/o dall'interno del *cyberspace* e poi elaborati. Un ambiente *hardware* e uno *software* sono indispensabili per l'interazione con l'esterno e l'esecuzione delle elaborazioni (cfr. voce *Intelligenza artificiale*, in *Treccani enciclopedia* online, https://www.treccani.it/enciclopedia/intelligenza-artificiale/). L'intelligenza artificiale è denominata così perché mira a imitare l'intelligenza e i comportamenti delle persone. Anch'essa rappresenta una tappa dello sviluppo della digitalizzazione, essendo il dibattito attualmente in corso dedicato all'individuazione dei limiti e rischi del ricorso alla super intelligenza in pochi anni. Questa si chiamerebbe in questo modo perché sarebbe in grado di superare l'intelligenza delle persone.

[3] L'integrazione dell'intelligenza artificiale nella sicurezza digitale può avere finalità eterogenee, in particolare 1. protezione avanzata contro attacchi informatici e violazioni dei dati; 2. miglioramento del rilevamento e della risposta alle minacce; 3. dipendenza ridotta dall'intervento umano; 4. tempi di ripristino più rapidi dopo attacchi alle infrastrutture e alla gestione dei dati; 5. conformità semplificata ai requisiti normativi.

[4] I rischi per la sicurezza digitale aggravati dall'uso di *software* fondati sull'intelligenza artificiale derivano dalla gestione di grandi quantità di dati in circolazione, molti dei quali sono sensibili o riservati, come le informazioni di identificazione personale ("*Personal Identification Information - PII*"). Attacchi alle infrastrutture e alla gestione dei dati e perdita di fiducia di clienti possono verificarsi qualora terzi riescano a sottrarre e/o manipolare dati siffatti. Rischi derivano altresì dalla mancanza di forza lavoro e dal divario di competenze, giacché esiste una carenza significativa di professionisti qualificati della sicurezza digitale. Questa carenza rende difficile la risposta agli incidenti ed evidenzia di per sé la necessità di soluzioni fondate sulla stessa intelligenza artificiale. Rischi possono derivare inoltre da attacchi di parti terze alla catena di fornitura di un'impresa o di un'organizzazione, quand'anche queste dispongano di misure adeguate di sicurezza digitale. Vulnerabilità possono essere generate da *partner*, fornitori e venditori di parti terze. Una strategia di sicurezza "globale" presuppone la gestione di questi rischi. Cfr., tra gli altri, G. SMORTO, *Il ruolo della comparazione giuridica nella contesa per la sovranità digitale*, in *DPCE* online, 2023, p. 339 ss.; B. FARRAND, H. CARRAPICO, A. TUROBOV, *The New Geopolitics of EU Cybersecurity: Security, Economy and Sovereignty*, in *International Affairs*, 2024, p. 2379 ss.; A. PIN, L. SCAFFARDI, *Tra protezione dei dati e intelligenza artificiale,* in *Europa e oltre*, in *DPCE* online, 2024, p. 1029 ss. Per un'analisi dei rischi suscettibili di porsi sul piano internazionale, si vedano S. BACKMAN, T. STEVENS, *Cyber Risk Logics and Their Implications for Cybersecurity*, in *International Affairs*, 2024, p. 2441 ss.

Essendo i rischi e le minacce posti da questi problemi di per sé senza confini, sorge il problema della ricerca, individuazione, preparazione e realizzazione di soluzioni comuni sul piano internazionale. Le risposte sono sovente di reazione e difesa. Soluzioni preventive sarebbero preferibili, ma risultano più improbabili perché la velocità degli sviluppi tecnologici mal si concilia con i rallentamenti della vita di relazione internazionale derivanti da divisioni e interessi differenti.

Gli sviluppi nel settore digitale, come tanti altri sorti dal progresso tecnico, si prestano in effetti a un uso positivo o avverso. Si caratterizzano dunque per un'utilizzazione duplice. La distinzione tra i due usi possibili – positivo o negativo – è chiara per alcune tecnologie, quale quella nucleare [5]. I due usi possibili non sono tuttavia predeterminabili, allorché si considerino le tecnologie e/o i *media* fondati sul processo di digitalizzazione e il funzionamento del loro spazio operativo, in sintesi, *cyberspace*, ossia uno spazio individuabile come insieme di *computer* in "rete" ovvero insieme di reti informatiche e infrastrutture fisiche, linguaggi e flussi di dati [6].

I rischi e le minacce derivanti dai possibili usi negativi dell'innovazione tecnologica digitale pongono inoltre problemi di sicurezza versatili e di difficile definizione. Nel diritto internazionale innovazione tecnologica e sicurezza digitale sono invero temi tra quelli di frontiera. L'esistenza di uno spazio digitale in quanto tale ha inciso, e incide, sull'accezione tradizionale di alcuni concetti di base del diritto internazionale, in particolare su quelli di sovranità, territorio, mezzi di minaccia e uso della forza, attribuzione dell'illecito internazionale, esercizio dei diritti delle persone e giurisdizione, applicabilità del diritto internazionale umanitario, nonché sui concetti di democrazia e sviluppo. È così che la ricerca di soluzioni comuni genera interrogativi

---

[5] La tecnologia nucleare può essere usata per la produzione di energia a uso civile e industriale in alternativa all'impiego di fonti fossili, mentre ha una capacità distruttiva macroscopica se usata a scopo militare. Rileva il parere reso, su richiesta dell'Assemblea generale delle Nazioni Unite, dalla Corte internazionale di giustizia l'8 luglio 1996 relativamente alla legalità della minaccia o dell'uso delle armi nucleari (*I.C.J. Reports*, 1996, p. 226 ss.).

[6] La cibernetica è qui intesa come la scienza volta allo studio e alla realizzazione del controllo e della regolazione, inclusa l'autoregolazione, della macchina, ossia un sistema complesso altamente organizzato di individuazione e analisi di dati eterogenei, mediante l'interazione e collaborazione tra settori di ricerca disparati e l'analogia tra i sistemi di comunicazione e regolazione della macchina e quelli degli organismi viventi. I settori più rilevanti sono ingegneria, fisica, biologia, insieme a psicologia, antropologia, sociologia ed economia. L'etimologia di cibernetica deriva dal greco "κυβερνητική" ("kybernētikē" sottinteso, "téchnē"), ossia "arte di pilotare". La cibernetica è la scienza dell'interazione uomo-macchina i cui principi di base sono *feedback*, controllo e comunicazione. Il *cyberspace*, comunemente inteso come *internet*, è un altro concetto inventato da William Gibson perché tutto sommato suonava bene, in confronto a *dataspace* o *infospace*, e adottato nel settore militare, a proposito soprattutto della sicurezza nazionale, e divenuto comunemente utilizzato in riferimento a *cyber attack*, *cyber threat*, *cyber operations*, *cybercrime/cybercriminal*, *cyberwarfare*, *cyberterrorism, cyber protection/defence* e *cyber security*. Cfr. A. WAGNER, N. ROSTOW, *Cybersecurity and Cyberlaw*, Carolina Academic Press, Durham, 2020, specialmente p. 3 ss.

su quali norme siano applicabili e/o possano esserlo in maniera indiretta, quali rimedi possano trovarsi e quali sviluppi normativi siano desiderabili [7].

Questo contributo ha per oggetto le risposte a problemi siffatti adottate e/o poste in essere dagli Stati attraverso le organizzazioni internazionali. Si intende individuare a quali problemi esse siano riuscite a dedicare più attenzione e con quale tipo di risposte, con riguardo alla loro portata sotto il profilo giuridico internazionale. Il contributo trae spunto dalle attività disparate di carattere non solo normativo, ma anche operativo delle organizzazioni internazionali. L'esame di quelle normative sarà centrale in quanto esse incidono sulla formazione e/o sullo sviluppo delle fonti applicabili e/o sui rimedi utilizzabili nel diritto internazionale, seppure talvolta indirettamente.

2. *Sicurezza digitale attraverso l'attività delle organizzazioni internazionali*

Negli anni Novanta, il *cyberspace* è stato un parametro di riferimento rilevante per il contrasto al ricorso e/o alla minaccia di usi della forza non convenzionali – fondati sul funzionamento di internet e dispositivi tecnologici e – la sorveglianza dell'interazione tra sicurezza internazionale e digitalizzazione. Dagli inizi di questo secolo, si è diffuso un interesse più ampio, a seguito del tasso di innovazione tecnologica sostenuto, della diffusione dell'uso di tecnologie e linguaggi digitali su larga scala, inclusi *software* fondati sull'intelligenza artificiale. Questi fenomeni hanno posto anche problemi di uso avverso della digitalizzazione nella sfera dei rapporti interindividuali, a seguito di fenomeni quali *interception* e *data collection*. Si è affermata altresì l'esigenza della sicurezza del commercio internazionale, ossia delle merci e servizi digitali transnazionali in circolazione, in particolare, come si segnalerà, di quelli fondati sull'intelligenza artificiale.

Più specificamente, l'insicurezza digitale ha rappresentato, e rappresenta, una minaccia o quantomeno un rischio nei rapporti tra Stati sul piano internazionale sotto tre profili. Il primo profilo è quello della pace e della sicurezza internazionale affinché le tecnologie digitali e/o internet non siano strumentali all'uso o alla minaccia del ricorso alla forza mediante mezzi non convenzionali e/o atti di terrorismo, in virtù del divieto dell'uso e della minaccia del ricorso alla forza nei rapporti internazionali e del principio di non interferenza negli affari altrui. Alla luce di questi parametri normativi riferibili al diritto internazionale generale, le tecnologie digitali e internet non dovrebbero essere usate neppure per attività di propaganda militare suscettibili di generare l'uso o la minaccia del ricorso alla forza armata. Il

[7] Cfr. A. WAGNER, N. ROSTOW, *op. cit.*, specialmente p. 1197 ss.; G. DELLA MORTE, *Limits and Perspectives of International Cyberspace Law*, in *Rivista di diritto internazionale*, 2022, p. 5 ss.

secondo profilo è quello del potenziamento dell'uso delle tecnologie digitali per la realizzazione dello sviluppo sostenibile mitigandone effetti avversi mediante, in particolare, l'osservanza dei diritti della persona, la trasparenza e la valorizzazione dell'etica nel processo di digitalizzazione. Questo profilo va associato a quello della stabilità politica e sociale negli Stati affinché l'uso delle medesime tecnologie non si accompagni a disinformazione intenzionale per interferenze in elezioni politiche, manipolazione dell'opinione pubblica e/o violazioni della riservatezza di dati e della vita privata delle persone. Il terzo profilo è quello del mantenimento della stabilità dell'economia di mercato e del regime di apertura e liberalizzazione del commercio internazionale, in quanto corollari della pace e della sicurezza internazionale. Esiste il problema della regolamentazione comune delle condizioni di ricorso a deroghe e/o barriere tecniche giustificate per condizionare l'uso delle tecnologie digitali a bilanciamenti concordati sul piano internazionale, al fine del potenziamento dei benefici e della riduzione dei rischi [8].

Tenuto conto dei tre profili di insicurezza digitale evidenziati, risposte comuni – vuoi normative vuoi operative – sono emerse, mediante la cooperazione internazionale istituzionalizzata ad opera delle organizzazioni internazionali, in relazione ad alcuni dei problemi comuni prospettati, in particolare rispetto alla sorveglianza e alla prevenzione di *cyber attacks* posti in essere da Stati, *State-sponsored actors* e/o privati nella forma di *cyberterrorism* e *cybercrime*; all'uso delle tecnologie digitali per la realizzazione dello sviluppo sostenibile; interferenze nei processi elettorali in sistemi di governo democratici, alla propaganda e disinformazione; e all'incidenza del processo di digitalizzazione sul commercio internazionale [9].

Per quanto concerne le risposte normative, non esiste un quadro giuridico multilaterale vincolante unitario, composto di regole materiali, procedurali e istituzionali specifiche. Si rilevano infatti diversi aspetti di frammentazione e "*international regulatory gaps*".

Le attività delle organizzazioni internazionali tendenzialmente universali hanno generato numerosi atti non vincolanti, esprimendo linee guida e orientamenti, sulla base anche di statistiche e infografiche. Gli atti non vincolanti delle organizzazioni internazionali tendenzialmente universali mirano, in via generale, all'armonizzazione e alla coerenza delle risposte normative e delle politiche nazionali, nonché alla gestione dei "vuoti", esaltando i benefici e mitigando gli effetti indesiderati del processo di digitalizzazione. Le organizzazioni internazionali hanno dedicato attenzione significativa alle situazioni di divario di sviluppo (*development challenges*) in

[8] La risoluzione dell'Assemblea generale delle Nazioni Unite n. 77/37 del 7 dicembre 2022 ricostruisce il quadro dei problemi e rischi generati dall'improprio utilizzo delle tecnologie di informazione e comunicazione.

[9] Cfr. T. MUNK, *The Rise of Politically Motivated Cyber Attacks: Actors, Attacks and Cybersecurity*, Routledge, Abingdon, Oxon, New York, 2022.

combinazione con il divario digitale derivante dalla diversa capacità degli Stati di creazione e impiego delle tecnologie informatiche più avanzate, come potenziate dai *software* fondati sull'intelligenza artificiale (*AI divide*).

Le organizzazioni internazionali hanno operato anche come fori di discussione tra gli Stati membri per la facilitazione della ricerca di soluzioni politiche e normative nazionali attraverso discussioni in seno alle rispettive istituzioni, l'adozione di *policy measures* e tentativi di avvio di negoziati per accordi internazionali relativi a problemi comuni specifici.

Tentativi di progettazione e creazione di norme specifiche sono stati fatti sul piano sia multilaterale tendenzialmente universale, soprattutto nel sistema delle Nazioni Unite, sia regionale dal Consiglio d'Europa e dall'Unione europea. A quest'ultima si farà cenno allorché opportuno, essendo questo scritto incentrato sulla prospettiva delle organizzazioni internazionali prive di competenze normative sovranazionali, a differenza dell'Unione. Le sue istituzioni possono adottare, com'è noto, atti normativi vincolanti e direttamente applicabili, *rectius* i regolamenti, sin dalla nascita della Comunità economica europea nel 1957, essendo il testo dell'articolo contemplante tale atto normativo – oggi l'art. 288 del Trattato sul funzionamento dell'Unione europea – rimasto invariato dal Trattato di Roma del 1957 a quello di Lisbona del 2007 attualmente in vigore.

Questo emerge pure dall'esame delle attività di organizzazioni internazionali regionali meno strutturate come quelle istituite tra Stati asiatici. Rilevano gli orientamenti sulla sicurezza digitale espressi dall'ASEAN ("*Association of Southeast Asian Nations*") per incoraggiare gli Stati parti a dotarsi di legislazioni nazionali in materia, realizzare attività di potenziamento della rispettiva "*capacity-building*", anche per la reazione a situazioni di emergenza digitale. Dal 2016 tali Stati si sono adoperati per l'adozione da parte dell'Associazione di regole comuni non vincolanti di coordinamento per la garanzia della sicurezza digitale in senso stretto, in quanto funzionale al mantenimento della pace e della sicurezza internazionale, richiamando quanto stabilito dall'"*UN Group of Governmental Experts*" (UNGE) [10] sul piano tendenzialmente universale relativamente, come si vedrà, all'applicabilità al *cyberspace* della Carta delle Nazioni Unite e dei suoi principi, quali la sovranità.

Per quanto concerne le risposte operative, le organizzazioni internazionali hanno svolto azioni, da un lato, di monitoraggio per il contrasto degli effetti pregiudizievoli della digitalizzazione, anche attraverso statistiche e indicatori, e, dall'altro, di assistenza tecnica tese alla valorizzazione e al potenziamento delle opportunità da essa generate secondo l'approccio unitario delle azioni per lo sviluppo sostenibile. Le azioni di assistenza tecnica hanno riguardato l'individuazione di problemi specifici e la ricerca di soluzioni al *digital divide* e quindi alle difficoltà di

[10] *Infra*, par. successivo.

mancanza di omogeneità delle condizioni di vita, occupazione, investimenti e innovazione ancora irrisolti tra Nord e Sud del mondo [11]. Il beneficio delle tecnologie digitali e dei *software* fondati sull'intelligenza artificiale implica infatti l'accesso a una rete internet veloce, la dotazione di infrastrutture, macchine e dispositivi appropriati, capacità finanziaria e tecnica per la produzione energetica, specialmente di elettricità, auspicabilmente con fonti rinnovabili, capacità di conservazione, gestione e ristoro dei dati. Per tali fini, diverse organizzazioni internazionali hanno raccomandato azioni di sicurezza digitale calibrate, presupponenti, tra l'altro, investimenti considerevoli in infrastrutture e risorse umane specializzate, programmi di istruzione e formazione adeguati, l'istituzione di *partnerships* a partecipazione pubblica e privata, suscettibili di stimolare la formazione di un quadro normativo specifico, in termini di finanziamenti, incentivi e risorse tecniche, da un lato, e procedure amministrative e programmi di formazione specializzata, dall'altro [12].

La diffusione di *software* fondati sull'intelligenza artificiale ha potenziato l'esigenza di norme e principi internazionali applicabili per la ricerca di soluzioni giuridiche ai problemi posti dalla realizzazione della sicurezza informatica.

Le organizzazioni internazionali si sono occupate di favorire risposte normative comuni sul piano internazionale nella logica precedentemente segnalata, promuovendo l'uso positivo dei *software* fondati sull'intelligenza artificiale e la mitigazione dei rischi. A tal fine, diverse organizzazioni internazionali si sono adoperate per l'individuazione dei caratteri distintivi dei suddetti *software*, evidenziando che i principi menzionati in precedenza, ossia non discriminazione, trasparenza, fiducia e sicurezza dell'uso dei dati personali nella prospettiva altresì della tutela della loro riservatezza (*privacy*), sono funzionali anche alla garanzia dell'attendibilità, nonché all'affidabilità (*trustworthy*), dell'uso dell'intelligenza artificiale. La diffusione dell'intelligenza artificiale ha accentuato invero la questione del rapporto tra *data governance* e *personal data protection*, ossia del bilanciamento tra innovazione e *privacy*. I *software* fondati sull'intelligenza artificiale necessitano di quantità ingenti di dati per l'addestramento. Questo genera problemi specifici di *privacy*, in termini di consenso e controllo delle informazioni personali racchiuse in tali dati. La tutela

---

[11] Cfr. E. SALTMAN, D. HUSSEIN, *Cyberspace and the Nouveau Colonialism*, in A. MHAJNE, A. HENSHAW (eds.), *Critical Perspectives on Cybersecurity: Feminist and Postcolonial Interventions*, Oxford University Press, Oxford, 2024, p. 52 ss.

[12] Rilevano le azioni delle Nazioni Unite, in particolare la "*Road Map for Digital Cooperation*" del Segretario generale (A/74/821, 20 maggio 2020). Tra gli istituti specializzati merita segnalare l'attività dell'UNESCO per quanto concerne le azioni volte alla mitigazione degli effetti avversi della combinazione tra divario di sviluppo e quello digitale. Segnalo altresì, tra gli altri, www.un.org/en/global-issues/artificial-intelligence; unitar.org/sustainable-development-goals/peace/our-portfolio/online-learning-and-education/ai-focussed-digital-cooperation-and-partnership-development-initiative.

dei diritti civili e politici riconducibili alla sfera della libertà personale, come la libertà di espressione può essere particolarmente compromessa dalla diffusione dell'intelligenza artificiale [13].

Versatilità di usi e adattabilità dei *software* fondati sull'intelligenza artificiale renderebbero difficile ideare e realizzare soluzioni normative fondate su previsioni e analisi dei rischi tese nel complesso alla prevenzione [14]. L'uso di tali *software* può risultare opaco perché certi requisiti tecnici di composizione dei prodotti e servizi ottenuti con *software* fondati su siffatta tecnologia sono riservati e protetti come tali, in quanto oggetto di diritti di proprietà intellettuale [15].

Nell'insieme le organizzazioni internazionali concordano, in linea di tendenza, sull'esigenza del ricorso a una "*trustworthy AI*", ossia sull'uso dell'intelligenza artificiale sulla base di fiducia, inclusione, accessibilità secondo equità, lealtà, trasparenza, tutela dei diritti della persona, dell'integrità delle informazioni e della riservatezza dei dati. Un'intelligenza artificiale siffatta sarebbe "robusta", in quanto diretta a un interesse pubblico, utilizzabile in sicurezza, con effetti prevedibili in maniera razionale, senza danni irreparabili, alterazioni dei comportamenti e delle opinioni reali. A tal fine, investimenti e *partnerships multistakeholder* sono considerati strumenti prioritari [16].

---

[13] Si segnala, tra gli altri, L. LANE, *Clarifying Human Rights Standards through Artificial Intelligence Initiatives*, in *International and Comparative Law Quarterly*, 2022 p. 915 ss.

[14] L'OCSE e l'OMC hanno pubblicato uno studio specifico nel 2024. Questo evidenzia, tra l'altro, come normative restrittive alla circolazione transnazionale di dati possano aumentare la fiducia, malgrado ciò possa implicare l'esclusione di alcuni usi dell'intelligenza artificiale e incidere quindi sulla riduzione dei costi da essa attesa. Si segnala già OECD, *Artificial Intelligence and International Trade. Some Preliminary Implications*, OECD Trade Policy Paper n. 260, aprile 2022.

[15] Talvolta i requisiti tecnici di composizione dei prodotti e servizi ottenuti con *software* fondati sull'intelligenza artificiale non sono comprensibili perché neppure chi ha contribuito alla programmazione e sviluppo di tali *software* può illustrarli in maniera articolata e completa. Pertanto, neppure la modalità *open source* potrebbe essere sufficiente per regolamentarne l'uso, onde mitigarne i rischi.

[16] Investimenti in ricerca e sviluppo di *software* di intelligenza artificiale sicuri e tesi alla soluzione di problemi internazionali comuni, come la realizzazione dello sviluppo sostenibile, sono raccomandati. Segnalo, tra gli altri, la "*Recommendation on the Ethics of Artificial Intelligence*", UNESCO, 2022; e l'"*Hiroshima AI Process* (HAIP)" avviato nel quadro del G7 nel 2023 e sostenuto dall'OCSE.

3. *La sicurezza digitale strumentale al mantenimento della pace e sicurezza internazionale, allo sviluppo sostenibile, alla tutela dei diritti della persona, all'attendibilità dell'informazione, alla stabilità dell'economia di mercato e del commercio internazionale, al tempo della diffusione dell'intelligenza artificiale*

Si propongono adesso alcune considerazioni in sub-paragrafi con riguardo a quanto concordato sul piano multilaterale tendenzialmente universale con riferimento ai tre profili di insicurezza digitale precedentemente menzionati.

a) Relativamente ai rischi per la pace e la sicurezza internazionale, le risposte normative sono state molteplici e hanno avuto per oggetto l'indicazione di linee di condotta comuni e l'istituzione di diversi organi consultivi di studio e ricerca. Giova dedicare attenzione alle risposte principali. Il Consiglio di sicurezza si è occupato di questa minaccia ampliando, negli anni successivi all'11 settembre 2001, la portata del concetto di terrorismo, altresì sulla base del nesso tra terrorismo e uso di internet [17], e il mandato del Comitato istituito nel 2001 contro il terrorismo (l'"*UN SC Counter-Terrorism Committee*") [18]. L'Assemblea generale si è occupata del tema dei "*Developments in the Field of Information and Telecommunications in the Context of International Security*" sin dal 1998 [19], promuovendo la nascita di alcuni organismi *ad hoc*, quali strumenti di difesa e reazione comune alle minacce potenzialmente derivanti dall'uso delle tecnologie informatiche, in particolare contro l'uso del *cyberspace* per la realizzazione di atti di terrorismo internazionale. Anzitutto, merita segnalare l'istituzione del Gruppo di esperti governativi delle Nazioni Unite (UNGE) – nominati dal Segretario generale della medesima organizzazione – nel 2004 per il potenziamento della pace e della sicurezza internazionale mediante l'individuazione di azioni di "confidence-building" in relazione al *cyberspace* [20].

---

[17] Rileva, in particolare, la risoluzione del Consiglio di sicurezza n. 2617/2021, S/RES/2617 (2021) del 30 dicembre 2021 relativamente alla desiderabilità di un approccio rispettoso dei diritti della persona e della "rule of law" relativamente al contrasto di atti di terrorismo posti in essere o minacciati mediante internet. Un approccio siffatto dovrebbe fondarsi sia sulla cooperazione internazionale sia sul ricorso a *partnerships* a partecipazione pubblica-privata con il coinvolgimento di rappresentanti delle imprese del settore delle tecnologie di informazione e comunicazione e della società civile.

[18] Il Consiglio di sicurezza ha istituito il Comitato contro il terrorismo con la risoluzione n. 1373/2001, S/RES/1373 (2001) del 28 settembre 2001, adottata a norma del Capo VII della Carta. Circa l'ampliamento del mandato di tale Comitato per la valorizzazione del collegamento tra internet e reclutamento, incitazione, pianificazione, realizzazione e finanziamento di atti di terrorismo, si segnala specialmente la risoluzione del Consiglio di sicurezza n. 2129/2013, S/RES/2129 (2013).

[19] Risoluzione UN Doc. A/RES/53/70 del 4 dicembre 1998.

[20] L'Assemblea generale ha istituito l'UNGE con la risoluzione n. 66/24, A/RES/66/24, del 2 dicembre 2011.

L'UNGE non è permanente. Hanno funzionato cinque diversi gruppi di esperti UNGE, concordando per l'applicabilità della Carta delle Nazioni Unite al *cyberspace*, sottolineando la desiderabilità di un *cyberspace* aperto, sicuro e accessibile e della condotta responsabile degli Stati e degli attori privati a tal fine conformemente al rispetto del principio di sovranità, dei diritti e delle libertà fondamentali della persona, come previsti nella Dichiarazione universale dei diritti dell'uomo e nei successivi Patti delle Nazioni Unite [21]. L'Assemblea generale ha istituito poi, tra gli altri, l'"*UN open-ended working group on Developments in the Field of Information and Telecommunications in the Context of International Security*" con la Risoluzione n. 73/27 del 2018 [22] e, al termine dei suoi lavori, dal 2021, un "*open-ended working group on security of and in the use of information and communications technologies 2021–2025*" sulla base della risoluzione n. 75/240 del 2020 [23] e un programma di azione per il potenziamento della condotta responsabile dello Stato nell'uso delle tecnologie di informazione e comunicazione con la risoluzione n. 77/37 del 2022 [24]. Altre iniziative operative degne di nota sono l'"*UN Global Counter-Terrorism Coordination Compact (UNGCTS)*" istituito nel 2018 dal Segretario generale delle Nazioni Unite nel quadro del processo di riforma delle azioni della suddetta organizzazione contro il terrorismo. Questo "*Compact*" ha un mandato esteso fondato tanto sul mantenimento della pace e della sicurezza internazionale quanto sullo sviluppo sostenibile, sui diritti della persona e affari umanitari *tout court*. Per la ricerca di approcci innovativi e il potenziamento della "*capacity-building*" degli Stati membri, in relazione alla prevenzione e alla reazione ad atti di terrorismo posti in essere mediante il *cyberspace*, rilevano altresì diverse attività dell'"*UN Office of Counter-Terrorism (UNOCT)*" nato nel 2017 ad opera dell'Assemblea generale delle Nazioni Unite [25]. Questo insieme all'UNCCT e all'INTERPOL ha istituito nel 2022 la "*CT Tech Initiative*" finanziata dall'Unione europea e tesa all'individuazione di possibili risposte coercitive e di giustizia penale. Rileva anche l'istituzione da parte del Centro di eccellenza sulla "*Cooperative Cyber Defence*" della NATO di un gruppo di esperti per la preparazione di un rapporto relativo all'individuazione, all'inquadramento sotto il profilo tecnico e giuridico e alla proposta di soluzioni in termini di diritto applicabile all'uso di tecnologie informatiche nella conduzione di operazioni militari.

---

[21] Per una valutazione dell'attività dell'UNGE nel quadro delle stesse Nazioni Unite, si veda UNODA, *Developments in the Field of Information and Telecommunications in the Context of International Security*, 2019 (consultabile *online* www.disarmament.unoda.org/ict-security). Cfr. P. GARGIULO, *The United Nations and Cybersecurity*, in *Cybersecurity Governance and Normative Frameworks. Quaderno La comunità internazionale*, 29, Editoriale scientifica, Napoli, 2024, p. 203 ss.

[22] A/RES/73/27 del 5 dicembre 2018.

[23] A/RES/75/240 del 31 dicembre 2020.

[24] A/RES/77/37 del 7 dicembre 2022.

[25] Si segnala la risoluzione n. 71/291 del 15 giugno 2017.

Questo gruppo ha pubblicato una prima edizione dei risultati della propria attività denominata "Manuale di Tallinn" nel 2013. Esso ha pubblicato la seconda edizione di tale "Manuale" nel 2017, al fine di precisare altresì gli effetti in tempo di pace dell'uso di tecnologie informatiche. Il gruppo di esperti ha concordato per l'applicabilità di principi e norme del diritto internazionale, in particolare quelli relativi alla non interferenza negli affari interni altrui, al divieto dell'uso e della minaccia della forza, al rispetto della sovranità, dei diritti della persona, delle immunità diplomatiche e consolari, del diritto internazionale umanitario, e della responsabilità quale conseguenza della violazione di obblighi internazionali [26]. Giova precisare che siffatto "Manuale" è una sorta di guida non vincolante sul piano tanto internazionale quanto interno. Esso rileva per il fatto che chiarisce la portata di principi e norme del diritto internazionale congegnati per rapporti interstatali di tipo convenzionale, evidenziando in particolare come gli Stati in quanto sovrani abbiano la responsabilità internazionale primaria di protezione dell'integrità dei propri sistemi informatici, in termini di dati e infrastrutture, e le norme internazionali, come quelle del diritto internazionale umanitario, trovino applicazione anche in situazioni di attacchi informatici e atti analoghi a danno di civili, infrastrutture militari e civili.

Il quadro operativo internazionalmente rilevante include anche l'"*hub*" su diritti della persona e tecnologie digitali istituito dal Segretario generale delle Nazioni Unite [27]. Secondo quanto da esso pubblicato la duplicità d'uso delle tecnologie digitali incide prevalentemente sull'esercizio dei diritti d'espressione, anche professionalmente come nel caso dei giornalisti, e riunione in luogo pubblico per manifestare opposizione politica in maniera non violenta, nonché sull'accesso effettivo all'istruzione senza discriminazioni.

b) Relativamente agli usi positivi della digitalizzazione per lo sviluppo, l'Organizzazione delle Nazioni Unite e suoi istituti specializzati hanno sottolineato come l'impiego dei risultati dello sviluppo tecnologico possa contribuire alla facilitazione della vita quotidiana delle persone e alla realizzazione dell'*Agenda 2030* sullo sviluppo sostenibile promossa dalle stesse Nazioni Unite [28]. Rilevano specialmente gli avanzamenti tecnologici, inclusi quelli fondati su *software* di intelligenza artificiale, suscettibili di favorire la prevenzione di emergenze – sanitarie e naturali –, e l'inclusività quale presupposto per l'attuazione effettiva degli obiettivi definiti dalla suddetta Agenda, detti SDGs dalla denominazione in lingua inglese (*Sustainable Development Goals*). Nel 2024 l'Assemblea generale delle Nazioni Unite ha preso una posizione chiara approvando la risoluzione intitolata "*Seizing the opportunities*

---

[26] Si veda M.N. SCHMITT (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge, Cambridge University Press, 2017. Cfr., tra gli altri, E.T. JENSEN, *The Tallinn Manual 2.0: Highlights and Insights*, in *Georgetown Journal of International Law*, 2017, p. 735 ss.

[27] digitalhub.ohchr.org/privacydata.

[28] Consultabile *online* (sdgs.un.org/2030agenda).

of safe, secure and trustworthy artificial intelligence systems for sustainable development" [29] e il "Global Digital Compact" [30]. Questo intende essere una "*roadmap for global digital cooperation*" – al fine del potenziamento dei benefici e della mitigazione del *digital divide* – dopo vent'anni dai tentativi della medesima Assemblea di perseguire lo stesso fine con la "*World Conference on International Telecommunication*" [31] e il "*World Summit on the Information Society*". La prima era volta alla discussione di revisioni del regolamento sulle telecomunicazioni dell'Unione internazionale delle telecomunicazioni ("*International Telecommunication Union*", anche nota come ITU), onde renderlo applicabile al processo di digitalizzazione. Il secondo mirava ad agevolare l'accesso, l'uso e la condivisione delle tecnologie per la comunicazione e l'informazione mediante una visione comune improntata alla garanzia dei diritti della persona e allo sviluppo sostenibile, essendo l'accesso a tecnologie siffatte da parte di uno Stato divenuto già a quel tempo un indicatore di misurazione della realizzazione di tale sviluppo [32]. Sviluppi ulteriori, in termini di conferenze ed eventuali negoziati sul piano multilaterale tendenzialmente universale, non hanno fatto seguito a questi tentativi dell'Assemblea generale. Lo spirito e l'intento di quei tentativi rimangono rilevanti, in quanto emergono, come evidenziato, nelle azioni recenti promosse nel quadro delle Nazioni Unite per la realizzazione dello sviluppo sostenibile anche attraverso lo sviluppo tecnologico. Prova ne è la risoluzione dell'Assemblea generale del 2024 sopra menzionata. Essa richiama alcuni principi in grado di assicurare l'uso responsabile e secondo "*due diligence*" [33] delle tecnologie digitali e dei *software* fondati sull'intelligenza artificiale, onde contribuire alla formazione di un quadro normativo aperto, accessibile, inclusivo e sicuro sul piano internazionale. I principi da essa valorizzati sono quelli

---

[29] Si veda la risoluzione dell'Assemblea generale delle Nazioni Unite n. A/78/L.49 del 21 marzo 2024.

[30] L'Assemblea generale delle Nazioni Unite ha adottato il "Global Digital Compact" il 22 settembre 2024 nel corso del "Summit of the Future" a New York dove i *leader* del mondo hanno adottato un "Pact for the Future".

[31] La "World Conference on International Telecommunication" si è tenuta a Dubai dal 3 al 14 dicembre 2012 (WCIT-12).

[32] Il "*World Summit on the Information Society*" è stata organizzato dalla Assemblea generale delle Nazioni Unite, sulla base della risoluzione n. 56/183 del 21 dicembre 2001, in due fasi: la prima a Ginevra dal 10 al 12 dicembre 2003 e la seconda a Tunisi dal 16 al 18 novembre 2005.

[33] La "due diligence" delle imprese di riferimento pare essere quella ancorata al rispetto dei diritti della persona. Meritano di essere segnalate due risoluzioni dell'Assemblea generale. La prima su "*Promotion and Protection of Human Rights in the Context of Digital Technologies*" del 22 dicembre 2023 (A/RES/78/213) e la seconda intitolata "*Artificial Intelligence Procurement and Deployment: Ensuring Alignment with the Guiding Principles on Business and Human Rights*" del 14 maggio 2025 (A/HRC/59/53) con cui l'Assemblea ha adottato il Rapporto del "*Working Group on the issue of human rights and transnational corporations and other business enterprises*" del Consiglio sui diritti dell'uomo.

riconducibili ai capisaldi dell'*Agenda 2030* per lo sviluppo sostenibile, in particolare ad alcuni dei SDGs. Si tratta degli obiettivi relativi all'equità nell'accesso ai programmi di istruzione, Obiettivo n. 4, e alla tutela della salute, Obiettivo n. 3, poiché l'impiego di tecnologie avanzate può contribuire alla mitigazione delle condizioni di accesso ai servizi di istruzione e sanitari primari, purché sia perseguito altresì l'obiettivo della riduzione delle diseguaglianze dentro ogni Stato e tra Stati, Obiettivo n. 10, con riguardo in particolare al problema del *digital divide*. L'impiego di processi produttivi tecnologicamente avanzati può agevolare inoltre la realizzazione degli obiettivi riconducibili alla tutela dell'ambiente *tout court*, in particolare l'assicurazione per tutti di "*availability and sustainable management of water and sanitation*", Obiettivo n. 6, e "*access to affordable, reliable, sustainable and modern energy*", Obiettivo n. 7.

Il perseguimento dello sviluppo sostenibile mediante la promozione degli usi positivi delle tecnologie digitali ha portato le organizzazioni internazionali a prevenire, nella misura del possibile, l'uso delle suddette tecnologie quali strumenti di disinformazione intenzionale, alterazione di processi elettorali e dell'opinione pubblica [34]. Queste azioni sono affini a quelle sulla promozione dello sviluppo sostenibile nell'osservanza dei diritti della persona, giacché sono finalizzate alla sostenibilità, in termini di attendibilità, dell'informazione e della comunicazione, mediante l'accessibilità secondo equità a informazioni verificabili e l'instaurazione di un clima di fiducia. La disinformazione può essere facilitata dalle tecnologie digitali, come potenziate dai *software* di intelligenza artificiale [35]. Per questa ragione, la prevenzione attraverso piani di alfabetizzazione digitale e il monitoraggio fondato sulla verificabilità delle informazioni ("*fact-checking*") sono ritenute due attività prioritarie.

Il contrasto della disinformazione posta in essere attraverso tecnologie digitali, in particolare piattaforme, si basa su risposte a intensità normativa forte nel diritto dell'Unione europea, in particolare dopo l'approvazione del Regolamento sul mercato interno per i servizi digitali del 19 ottobre 2022 (noto come "*Digital Service Act*", DSA) in vigore dal 17 febbraio 2024 [36]. Questo istituisce, tra l'altro, una sorta di controllo congiunto da parte delle istituzioni europee e degli stessi gestori delle piattaforme – detta "coregolamentazione" – secondo cui la Commissione europea

---

[34] Cfr., tra gli altri, D. STEIGER, *International Law and New Challenges to Democracy in the Digital Age: Big Data, Privacy and Interferences with the Political Process*, in N. WITZLEB, J. RICHARDSON, M. PETERSON (eds.), *Big Data, Political Campaigning and the Law: Privacy and Democracy in the Age of Micro-Targeting*, Routledge, Abingdon, Oxon, New York, 2020, p. 71 ss.

[35] Si veda, tra gli altri, J. KENNY, *Advanced Artificial Intelligence Techniques and the Principle of Non-Intervention in the Context of Electoral Interferences*, in F. CRISTIANO AND OTHERS, *Artificial Intelligence and International Conflict in Cyberspace*, Routledge, Abingdon, Oxon, New York, 2023, p. 223 ss.

[36] Regolamento (UE) n. 2022/2065 sul mercato interno per i servizi digitali, in *GUUE* L 277, 27 ottobre 2022, p. 1 ss. Esso è entrato in vigore il 17 febbraio 2024.

può vincolare un gestore a realizzare attività di "fact-checking", qualora questi non lo faccia adeguatamente soprattutto sotto il profilo procedurale [37]. La base normativa del Regolamento è l'art. 114 del Trattato sul funzionamento dell'Unione europea. Si tratta come noto di una base flessibile e strumentale al "buon funzionamento del mercato interno". Questo resta lo scopo prevalente dell'Agenda digitale dell'Unione europea, quantunque nella logica valoriale caratterizzante, in linea di principio, l'azione dell'Unione. In effetti, essa ha un'agenda articolata contro la disinformazione digitale. Oltre al codice di buon pratiche contro la disinformazione per i gestori di piattaforme digitali – indirettamente rilevante nell'attuazione del Regolamento DSA – l'Unione ha adottato atti tesi al potenziamento e alla valorizzazione del processo di democratizzazione, mediante la garanzia del pluralismo, da un lato, *ex* art. 10 del Trattato sull'Unione europea, e l'integrità e correttezza delle informazioni alla base della libertà di espressione, come previsto all'art. 11 della Carta dei diritti fondamentali dell'Unione stessa [38]. Il controllo del rispetto della normativa del Regolamento dipende da un meccanismo istituito *ad hoc* – l'*European Board for Digital Services* [39] – e dall'attività di sorveglianza della stessa Commissione europea [40]. La giurisdizione della Corte di giustizia dell'Unione europea a conoscere e pronunciarsi sui ricorsi relativi alla violazione e alla validità del diritto dell'Unione *tout court* è un'opzione altresì aperta nelle circostanze del caso.

Il diritto internazionale non contempla risposte normative così calibrate per il contrasto della disinformazione e garantite da una certa effettività. Significativi sono tuttavia alcuni rapporti della *Special Rapporteur* sulla libertà di opinione ed espressione dell'Alto Commissariato delle Nazioni Unite sui diritti dell'uomo [41]. Qui sono richiamati la "resilienza sociale" [42], l'osservanza dei diritti della persona e

---

[37] Rileva specialmente l'art. 37 del Regolamento relativamente ai "fornitori di piattaforme online di dimensioni molto grandi o del motore di ricerca online di dimensioni molto grandi".

[38] Rilevano, in particolare, il "Piano d'azione per la democrazia europea" del 2020, il pacchetto per la difesa della democrazia del 2023 fino allo "Scudo europeo della democrazia" annunciato dalla presidente della Commissione, Ursula von der Leyen durante la campagna per la sua rielezione nel 2024 e le norme dell'Unione sul rafforzamento della democrazia per la promozione di elezioni libere ed eque, l'accrescimento della trasparenza nella propaganda politica e il rafforzamento dei diritti elettorali del 2024. Cfr. P. CAVALIERE, *Freedom of Expression after Disinformation: Towards a New Paradigm for the Right to Receive Information*, in *Journal of Media Law*, 2024, p. 1 ss.

[39] Segnalo articoli 61 ss. del Regolamento.

[40] Rilevano articoli 66 ss. del Regolamento.

[41] Si vedano, in particolare, il rapporto su "*Gendered disinformation and its implications for the right to freedom of expression*", A/78/288, del 7 agosto 2023, quello su "*Disinformation and freedom of opinion and expression during armed conflicts*", A/77/288, del 12 agosto 2022 e il discorso della *Special Rapporteur* al Consiglio delle Nazioni Unite sui diritti dell'uomo su "*Disinformation and freedom of opinion and expression*", A/HRC/47/25, del 13 aprile 2021.

[42] L'espressione "resilienza sociale" è divenuta ricorrente durante la pandemia da Covid-19 per

l'approccio *multistakeholder*, fondato sulla partecipazione di imprese e rappresentanti della società civile, quali strumenti di contrasto della disinformazione sul piano internazionale. L'Assemblea generale e il Segretario generale delle Nazioni Unite hanno contribuito anch'essi a delineare siffatto approccio pubblicando risoluzioni e strategie di azione mirate [43].

c) Vari aspetti delle dinamiche alla base dell'economia di mercato e del commercio internazionale sono esposti ad alcuni rischi specifici di alterazione derivanti dalla diffusione dell'intelligenza artificiale. L'ampia circolazione per usi disparati dei *software* fondati su questa tecnologia avanzata rende di per sé opportuna l'adozione di politiche anche commerciali calibrate per numerosi Stati, in virtù dell'aumento del rischio di "rimanere indietro" [44]. L'"*AI Advisory Body*" delle Nazioni Unite ha evidenziato invero come il divario di capacità di produzione e gestione dei *software* fondati sull'intelligenza artificiale possa accentuare complessità e vulnerabilità della *data driven economy* e alterare le condizioni di efficacia del diritto e della politica sul piano interno [45].

Gli atti normativi non vincolanti in materia delle organizzazioni internazionali mirano così a indirizzare gli Stati membri nella scelta di quali misure politiche e normative siano più desiderabili e nell'impostazione di "*capacity and confidence building partnerships*" tra Stati, imprese e società civile giacché il ricorso all'approccio *multistakeholder* teso alla prevenzione è desiderabile anche a questo fine. Gli orientamenti espressi dalle organizzazioni internazionali denotano inoltre la probabilità di ostacoli all'efficacia delle normative e politiche in materia di concorrenza [46]. Per

---

sottolineare l'esigenza dello sviluppo delle abilità di gruppi e comunità di gestire l'esposizione a situazioni di pressione avversa a seguito di cambiamenti ambientali, politici e sociali. Si veda, tra gli altri, la "*UN Common Guidance on Helping Build Resilient Societies*" del 2020 (consultabile *online*). Segnalo che il tema della "*community based resilience*" era oggetto già di azioni delle Nazioni Unite per la realizzazione dello sviluppo sostenibile precedentemente alla suddetta pandemia.

[43] Segnalo, in particolare, "*United Nations Strategy and Plan of Action on Hate Speech*" pubblicato dal Segretario generale il 18 giugno 2019 e la risoluzione dell'Assemblea generale n. 76/227, A/RES/76/227, del 24 dicembre 2021 su "*Countering Disinformation for the Promotion and Protection of Human Rights and Fundamental Freedoms*".

[44] La maggior parte dei brevetti di *software* fondati sull'intelligenza artificiale sono registrati in Cina, in misura minore in Canada, Giappone e Stati Uniti e poi nella Repubblica di Corea. Cfr. L. TREMOLADA, *La Cina ha più brevetti degli Stati Uniti in intelligenza artificiale. Cosa vuol dire?*, in *Il Sole 24 ore*, 4 luglio 2024.

[45] Si veda, in particolare, il rapporto dell'"AI Advisory Board" pubblicato nel settembre 2024 intitolato "*Governing AI for Humanity*" (consultabile *online*). Cfr. W. HOFFMANN-RIEM, *Artificial Intelligence as a Challenge for Law and Regulation*, in T. WISCHMEYER, T. RADEMACHER (eds), *Regulating Artificial Intelligence*, Springer, Cham, 2020, p. 1 ss.

[46] La diffusione dell'uso di algoritmi può accompagnarsi a concentrazioni industriali volte all'esclusione dei concorrenti dal mercato e ad altre pratiche anticompetitive. Le organizzazioni a vocazione economica, tra cui OCSE e Unione europea, sono quelle più attive in materia probabilmente per il

questo un'altra azione desiderabile per la prevenzione sarebbe l'adozione di politiche di concorrenza comuni, in luogo di interventi reattivi *ex post* unilaterali diversificati sul piano nazionale e suscettibili di effettività incerta, specialmente ad opera di Stati economicamente meno avanzati. Risposte comuni sulla tutela dei diritti di proprietà intellettuale, in particolare del *copyright*, in relazione a scoperte fondate sull'intelligenza artificiale sono altresì raccomandate [47]. L'osservanza degli strumenti normativi internazionali sulla tutela dei diritti della persona ha poi una rilevanza speciale, in relazione alla diffusione dell'intelligenza artificiale, per la tutela dei diritti economici e sociali di lavoratori o altre persone suscettibili di essere da essa danneggiate per effetto della sostituzione delle persone con umanoidi, per esempio, alle catene di produzione; di esperti, come i traduttori di lingua straniera e avvocati, con *automated legal advice tools*; o per effetto del rapporto di dipendenza tra professioni nuove, quali autisti *Uber* e *riders*, e algoritmi.

Le organizzazioni internazionali concordano inoltre sull'opportunità del contemperamento dell'esigenza di tutela rafforzata della riservatezza dei dati personali, derivante dalla capacità gestionale e predittiva notevole degli algoritmi, e l'interesse dei gestori di piattaforme e flussi di dati alla libera circolazione. Normative sulla *privacy* "robuste", per quanto incoraggiate, possono vanificare infatti, in via generale, le opportunità derivanti dagli scambi commerciali generati o quantomeno promossi dall'intelligenza artificiale. Tali normative possono essere un ostacolo per le attività dei gestori di piattaforme, se rendono meno attrattive per esempio le *apps* fondate sull'intelligenza artificiale. L'esigenza di un contemperamento tra i suddetti interessi emerge soprattutto dagli atti di organizzazioni internazionali a vocazione economica. Rilevano i Principi in materia adottati dall'OCSE già nel 2019 per indicare agli Stati membri soluzioni normative e politiche per la mitigazione dei rischi e la diffusione di *software* di intelligenza artificiale affidabili [48].

Gli orientamenti menzionati sono funzionali alla ricerca di soluzioni al problema della mitigazione dei rischi anche nel diritto del commercio internazionale relativamente al commercio di prodotti e servizi fondati sull'intelligenza artificiale [49].

---

fatto che i loro Stati membri sono, in linea di tendenza, Stati economicamente avanzati. Cfr. OECD, *Artificial Intelligence, Data and Competition*, Working Paper, 24 maggio 2024; OECD, *Handbook on Competition Policy in the Digital Age*, Paris, 2022. Approfondimenti sono reperibili online nel sito dell'OCSE (in particolare, oecd.org/en/topics/competition-and-digital-economy.html). Per l'orientamento dell'Unione, segnalo, tra gli altri, "*Speech by EVP Margrethe Vestager at the European Commission workshop on 'Competition in Virtual Worlds and Generative AI*", 28 giugno 2024.

[47] Cfr. S. CHENG PENG, *Artificial Intelligence and Copyright: the Authors' Conundrum*, in WIPO-WTO Colloquium papers, 2018, p. 173 ss.

[48] Per approfondimenti e aggiornamenti sull'applicazione dei Principi da parte degli Stati membri dell'OCSE, si veda il sito internet della medesima organizzazione (oecd.org).

[49] Il 21 novembre 2024 l'OMC ha pubblicato il rapporto "*Trading with Intelligence: How AI Shapes and Is Shaped by International Trade*" per illustrare la correlazione tra commercio e intelligenza

Rilevano in particolare le attività dell'Organizzazione mondiale del commercio (OMC). L'intenzione dell'OMC pare essere di promuovere lo sviluppo e la diffusione di *software* fondati sull'intelligenza artificiale, potenziandone le opportunità e mitigandone i rischi cui paesi in via di sviluppo e piccole-medie imprese sono maggiormente esposti, anche perché la concentrazione industriale caratterizza la produzione di tali *software*. Il Comitato dell'OMC sugli ostacoli tecnici al commercio (TBT) si è focalizzato sulle "*cybersecurity-related TBT measures*" specificamente dal 2022, giacché ostacoli tecnici si prestano a essere introdotti per il controllo della sicurezza di tali *software*.

L'OMC vuole essere un foro multilaterale di discussione, negoziati e *rule-making* per quanto concerne la rilevanza del commercio internazionale nelle *governance* della intelligenza artificiale, la ricerca di un "*globally coordinated approach*" e della coerenza delle risposte statali, a fronte della diversificazione tra le eventuali normative applicabili ai prodotti fondati sull'intelligenza artificiale. Secondo l'OMC, l'armonizzazione operativa e normativa gioverebbe alla partecipazione al commercio internazionale di paesi in via di sviluppo e piccole-medie imprese, grazie alla riduzione dell'incidenza delle barriere tecniche e dei costi, a fronte del probabile vantaggio che gli Stati economicamente avanzati avranno in futuro, in virtù degli aumenti presumibili dei tassi di innovazione e produttività generati dall'intelligenza artificiale in una prospettiva ipotetica fino al 2040 [50].

4. *Le organizzazioni internazionali regionali di fronte alla diffusione della tecnologia digitale, in particolare dell'intelligenza artificiale*

La ricerca del diritto internazionale vincolante in materia di cybersicurezza ha risultati a intensità normativa più forte sul piano regionale, allorché si considerino le attività del Consiglio d'Europa. Esso ha promosso invero la conclusione di alcuni accordi internazionali speciali relativamente sia all'uso criminale delle tecnologie digitali sia alle esigenze di tutela dei diritti della persona generate dal loro uso *tout court*.

Le Convenzioni del Consiglio d'Europa sono strumenti normativi con un ambito di applicazione circoscritto non solo *ratione personae*, ma anche *ratione materiae*,

---

artificiale in quanto "*trade issue*", evidenziando quanto questa tecnologia sia destinata a trasformare radicalmente il modo in cui si lavora, si produce e si commercia. Essa può ridurre i costi del commercio internazionale relativi alla logistica grazie, per esempio, a sistemi di automazione e predizione dei rischi, alla gestione razionale delle catene globali del valore, alla ristrutturazione dei servizi, all'aumento del commercio in "*AI-related goods and services*" e alla ridefinizione dei vantaggi comparativi delle economie, stante la diversificazione tra le eventuali normative a essa applicabili.

[50] Stima di crescita del commercio reale del 14% in una visione ottimistica, oppure del 7% in una visione pessimistica, cui si associa la stima di crescita dei servizi digitali pari al 18% in una visione ottimistica (WTO, *op. cit.*, specialmente pp. 4-5, 7).

ideati a vantaggio della tutela dei diritti delle persone, della democrazia e della "*rule of law*". Sono le prime normative settoriali vincolanti sul piano internazionale relativamente all'uso del *cyberspace* secondo regole comuni. Si tratta della Convenzione n. 108/1981 del 28 gennaio 1981 sulla protezione delle persone rispetto al trattamento automatizzato dei dati personali e il suo successivo Protocollo del 2018 volto ad "avvicinare" il regime normativo della Convenzione al Regolamento dell'Unione europea su trattamento e circolazione dei dati personali [51]. Il regime normativo della Convenzione è stato innovativo, quando negoziato, perché ha rappresentato la prima disciplina internazionale tesa a coniugare libera circolazione transnazionale dei dati, libertà di informazione, garanzia del diritto alla vita privata e di altri diritti e libertà fondamentali della persona. L'art. 2 della Convenzione denota lo sforzo degli Stati contraenti di definire alcuni concetti tecnici controversi allorché regimi di libertà eterogenei siano in gioco, quali le definizioni di "dati a carattere personale", "collezione automatizzata di dati", "trattamento automatizzato" e "detentore di una collezione di dati". La Convenzione richiama alcuni principi, quali parametri di riferimento della disciplina comune del trattamento automatizzato di dati personali, al fine della garanzia della "qualità dei dati" in circolazione [52]. Questi principi sono legalità, trasparenza e correttezza dell'uso dei dati rispetto ai fini.

La Convenzione sul "cybercrime" del 2001 è stata la prima normativa vincolante volta a introdurre obblighi per gli Stati sul piano internazionale relativamente

---

[51] Regolamento (UE) n. 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati del 27 aprile 2016 (in *GUUE*, L 119, 4 maggio 2016, 1 ss.) ed entrato in vigore il 25 maggio 2018. Merita osservare che l'Unione europea ha inteso col Regolamento disporre di uno strumento normativo funzionale al ruolo di "*global standard setter*" anche nel campo della circolazione transnazionale di dati per motivi commerciali e/o di "law-enforcement". Rileva specificamente, il suo "*adequacy approach*", fondato sull'art. 45 del Regolamento, nella misura in cui esso funga da "global standard" per una sorta di "*Brussels effect*" in questo campo. In breve, la Commissione europea ha la competenza di determinare se uno Stato terzo offra un livello adeguato di protezione dei dati. L'adozione di una decisione positiva su siffatta adeguatezza presuppone l'espletamento di una procedura articolata fondata sulla partecipazione di più organi dell'Unione e indirettamente degli Stati membri: una proposta della Commissione europea, il parere favorevole dell'"*European Data Protection Board*", l'approvazione dei rappresentanti degli Stati membri dell'Unione, l'adozione della decisione della Commissione europea. Cfr. S. SALUZZO, *The EU as a Global Standard Setting Actor: the Case of Data Transfers to Third Countries*, in E. CARPANELLI, N. LAZZERINI, *Use and Misuse of New Technologies,* Springer Nature, Cham, 2019, p. 115 ss.; W. PANEK, *The European Commission's Adequacy Decisions' Content as a Guide for Applying the Adequacy Assessment Criteria*, in J.H. HOEPMAN, M. JENSEN, M.G. PORCEDDA, S. SCHIFFNER, S. ZIEGLER (eds), *Privacy Symposium 2024*, Springer, Cham, 2025, p. 23 ss.

[52] Art. 5 della Convenzione n. 181/2001. Il Protocollo alla Convenzione non è in vigore. Per approfondimenti sull'attività del Consiglio d'Europa in questo settore, si vedano I. INGRAVALLO, E. DRAGO, *The Council of Europe's Actions in the Field of Cybersecurity*, in *Cybersecurity Governance and Normative Frameworks*, cit., p. 203 ss.

all'uso del *cyberspace*, attraverso il bilanciamento tra ricorso a misure restrittive dell'accesso a internet eventualmente adottate dagli Stati contraenti, per la prevenzione e repressione di reati commessi tramite internet e la tutela dei diritti della persona rilevanti, quali quello della libertà di espressione. Questa Convenzione mira all'armonizzazione del diritto penale nazionale degli Stati contraenti avente per oggetto alcuni reati commessi tramite internet. La Convenzione si riferisce ai reati di violazione dei diritti d'autore, frode informatica, pornografia infantile e violazione della sicurezza della rete, prevedendo come rimedi la perquisizione dei sistemi di reti informatiche e l'intercettazione dei dati. Essa rileva altresì per le definizioni tecniche di sistema informatico ("*computer system*"), dati informatici ("*computer data*"), fornitore di servizi ("*service provider*") e trasmissione di dati ("*traffic data*") contemplate all'art. 1. Significativo altresì il rinvio da essa previsto, tra gli altri, alla Convenzione europea sui diritti dell'uomo conclusa nel quadro dello stesso Consiglio d'Europa, come noto, già nel 1950, e al Patto delle Nazioni Unite sui diritti civili e politici del 1966 per quanto concerne la tutela dei diritti della persona. Relativamente al contrasto del "cybercrime" merita segnalare altresì la relativa Convenzione adottata il 31 dicembre 2024 dall'Assemblea generale delle Nazioni Unite [53]. Questa prevede norme di diritto penale comune di portata ampia che gli Stati parti sono obbligati ad attuare nei propri ordinamenti, in quanto responsabili primari dell'effettività delle azioni internazionali contro il "cybercrime", favorendo altresì il ricorso a un approccio *multistakeholder* teso alla prevenzione [54]. L'obbligo di dotarsi di strumenti di sorveglianza elettronici utilizzabili "in tempo reale" posto dalla Convenzione agli Stati parti [55] e la possibilità estesa di accesso ai dati personali delle persone ammessa dalla stessa [56] mirano al potenziamento della sorveglianza contro il "cybercrime". Si ravvisa l'esigenza dell'interazione bilanciata tra disposizioni siffatte e la tutela di taluni diritti della persona, quali quelli concernenti la libertà di espressione e la salvaguardia della riservatezza dei dati personali, come osservato già in dottrina, considerato il fatto che la Convenzione menziona espressamente la tutela dei diritti della persona quale parametro di riferimento, agli artt. 6 e 24 [57]. La Convenzione

---

[53] La Convenzione delle Nazioni Unite contro il "cybercrime" è volta a "*Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes*". Si veda la risoluzione dell'Assemblea generale A/RES/79/243 del 31 dicembre 2024.

[54] La portata ampia degli obblighi posti dalla Convenzione deriva anzitutto dall'ampiezza dei crimini informatici da essa previsti, tra cui, i reati di accesso a dispositivi digitali altrui, "interception", violazione dei diritti d'autore, frode informatica, pornografia infantile e violazione della sicurezza della rete.

[55] Art. 29.

[56] Art. 28.

[57] Si veda F. SEATZU, *The New UN Convention on Cybercrime: Between Securing Cyberspace and*

contempla sanzioni come il congelamento e la confisca dei risultati dell'attività illecita, delle macchine e di altri strumenti usati per la realizzazione di una attività siffatta [58], l'eventualità dell'estradizione [59] e obblighi procedurali di scambio di informazioni [60], assistenza tecnica e cooperazione internazionale per l'armonizzazione delle capacità di attuazione delle proprie disposizioni da parte degli Stati parti [61].

Il Consiglio d'Europa ha favorito inoltre la conclusione della Convenzione quadro su intelligenza artificiale, diritti della persona e "*rule of law*" nel 2024. Si svolgeranno considerazioni specifiche su questa Convenzione nel prosieguo.

Con riguardo all'attitudine degli organismi regionali istituzionalizzati, l'Unione europea ha adottato diversi strumenti per lo sviluppo di *software* di intelligenza artificiale affidabili, tra cui, il 24 gennaio 2024 l'"*AI Innovation Package*" a sostegno finanziario e tecnologico di piccole-medie imprese e "*startups*". Già nel 2018 l'Unione aveva adottato il Piano coordinato sull'intelligenza artificiale" ("*Coordinated Plan on AI*") teso a promuovere investimenti, la realizzazione di strategie e programmi calibrati dell'Unione e mitigare fenomeni di diversificazione. Questo include il regolamento sull'intelligenza artificiale (AI Act) del 2024 volto a favorire l'impiego di sistemi di intelligenza artificiale "robusti", in quanto affidabili, suscettibili di adattamento a imprevisti e operatività anche in contesti incerti, nell'eventualità di errori e/o imprevisti, caratterizzati da vulnerabilità bassa, fondati su innovazione responsabile, trasparenza nell'individuazione, analisi e gestione dei rischi [62]. Il Regolamento intende garantire in proposito i diritti fondamentali della persona e i valori dell'Unione europea.

Come menzionato, rileva poi che nel 2024 il Consiglio d'Europa abbia adottato la convenzione quadro su intelligenza artificiale, diritti della persona, democrazia e "Rule of Law" ("*Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law*") diretta a rispondere ad alcuni degli interrogativi menzionati. La Convenzione definisce, all'art. 2, l'intelligenza artificiale come "*a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations or*

Undermining Fundamental Rights and Freedoms, in *La Comunità internazionale*, 2025, p. 227 ss. Cfr. M. DIMETTO, *Convenzione delle Nazioni Unite contro il* cybercrime *e tutela dei diritti umani: influenze europee sullo scenario internazionale*, in *Freedom, Security, Justice*, 2025, n. 2, p. 108 ss.

[58] In particolare, art. 31.

[59] Art. 37.

[60] Art. 55.

[61] Artt. 54 e 56.

[62] Regolamento (UE) n. 2024/1689 del 13 giugno 2024, in *GUUE* L del 12 luglio 2024, entrato in vigore il 1° agosto 2024. Per alcuni approfondimenti sul quadro normativo di riferimento precedentemente all'adozione del suddetto Regolamento, si veda C. GRIECO, *Intelligenza artificiale e tutela degli utenti nel diritto dell'Unione europea*, Editoriale scientifica, Napoli, 2023.

decisions that may influence physical or virtual environments. Different artificial intelligence systems vary in their levels of autonomy and adaptiveness after deployment". Si tratta di una definizione squisitamente tecnica. Essa pone poi agli Stati parti obblighi funzionali all'osservanza dei diritti della persona, inclusi quelli sulla riservatezza del trattamento dei dati, integrità e correttezza dei processi democratici, sulla non discriminazione, sulla trasparenza, sull'*accountability*, sull'innovazione responsabile e attendibilità. Altri organismi regionali si sono occupati di associare l'uso dell'intelligenza artificiale all'osservanza dei diritti della persona e dell'etica [63] o di redigere documenti quadro in materia, come il "*2024 African Union Development Agency-New Partnership for Africa's Development (AUDA-NEPAD) White Paper*" e l'"*African Union Continental Artificial Intelligence Strategy*" [64].

Sul piano meno istituzionalizzato, merita segnalare l'attenzione anche nel quadro G7/G20 alla redazione di orientamenti di macrosistema per le applicazioni dell'intelligenza artificiale, secondo numerosi parametri già menzionati, ossia inclusività, non discriminazione, "*open access*", sostenibilità, attendibilità e trasparenza [65].

5. *Considerazioni conclusive*

Le attività e gli orientamenti delle organizzazioni internazionali traggono spunto dalla potenziale duplicità delle finalità d'uso del *cyberspace* e si fondano su un approccio "*risk-based*". Il processo di digitalizzazione è caratterizzato positivamente se sostenibile, ossia volto alla democraticità, in termini di partecipazione e pluralismo, all'integrazione tra interessi eterogenei, trasparenza, innovazione razionale e responsabile. Esso è considerato sfavorevolmente se usato per l'uso o la minaccia della forza da parte di Stati o attori da essi sponsorizzati, atti di criminalità informatica, interferenze distorsive in processi elettorali e nel commercio internazionale.

Ciò può assumersi sulla base di diverse attività tanto normative quanto operative delle organizzazioni internazionali in riferimento all'esigenza comune di sicurezza digitale.

Per quanto concerne i risultati principali delle attività normative, indipendentemente dalla loro natura vincolante o meno, merita segnalare in particolare le

---

[63] Segnalo, in particolare, la "2023 Southern Common Market (MERCOSUR) Ministerial Declaration on the Principles of Human Rights in the Field of Artificial Intelligence" e la "2024 ASEAN Guide on AI Governance and Ethics".

[64] La "Strategia" dell'Unione africana individua quattro settori prioritari: agricoltura, assistenza sanitaria, istruzione e adattabilità al cambiamento climatico.

[65] Merita menzionare il "*Ministerial Statement*" su commercio ed economia digitale adottato nel quadro del G20 nel 2019, insieme al "*G7 Hiroshima Process on Generative AI*" del 2023 e gli "*AI Guiding Principles and AI Code of conduct*" del G7 dello stesso anno.

risoluzioni del Consiglio di sicurezza, quelle numerose dell'Assemblea generale, le convenzioni internazionali promosse dal Consiglio d'Europa, i regolamenti dell'Unione europea, i principi dell'OCSE e di altri organismi internazionali regionali. L'interesse principale pare essere il funzionamento dello spazio digitale secondo regole e principi comuni. Le attività normative mirano, nella misura del possibile, al coordinamento della gestione di infrastrutture e di dati; all'armonizzazione, là dove esistano risposte normative nazionali; alla promozione della creazione di norme comuni di regolamentazione dei rischi e delle minacce generati dallo sviluppo tecnologico digitale; alla garanzia della tutela dei diritti della persona e della trasparenza; e alla diffusione di *best practices*. Nell'insieme l'obiettivo di macrosistema appare essere quello della promozione di uno spazio digitale accessibile, aperto, prevedibile, stabile e sicuro funzionale alla pace e sicurezza internazionale e alla garanzia dei diritti della persona attraverso l'applicazione del diritto internazionale e la creazione, nella misura del possibile, di norme specifiche sulla condotta degli Stati, degli attori da essi sponsorizzati, dei gestori e degli utenti delle piattaforme digitali.

Non emergono risposte normative omogenee. I risultati sono di natura disparata – vincolante o meno ovvero di portata multilaterale o "regionale" – e suscettibili per questo di incidere in maniera non coerente sulla vita di relazione internazionale.

Per quanto concerne i risultati principali delle attività operative poste in essere e/o promosse da organizzazioni internazionali, numerose di esse concordano che la rapidità dei mutamenti tecnologici presupponga risposte "robuste", da un lato, e suscettibili di adattarsi alla realtà, dall'altro. Rilevano le attività di assistenza tecnica a beneficio degli Stati membri, quali attività di *capacity-building* e *confidence-building* per la realizzazione dell'uguaglianza effettiva, malgrado le differenze di sviluppo socioeconomico e tecnologico, nel rispetto della sovranità statale; coordinamento, orientamento e facilitazione della loro cooperazione.

Possono svolgersi considerazioni finali ulteriori.

Primo, il contrasto dell'uso avverso delle tecnologie digitali ha un' intensità normativa specifica più forte per la risposta ad alcuni rischi – come la rottura o la minaccia alla pace e sicurezza internazionale e la violazione di diritti della persona –, mentre ha una intensità inferiore relativamente ad altri usi avversi, quali l'interferenza nei processi elettorali, la propaganda e la disinformazione.

Secondo, i parametri normativi internazionali di riferimento prioritari sono gli obblighi e i principi della Carta delle Nazioni Unite, in particolare quelli di uguaglianza sovrana degli Stati, divieto dell'uso e della minaccia dell'uso della forza contro l'integrità territoriale e indipendenza politica degli Stati, la non interferenza negli affari altrui, la soluzione pacifica delle controversie e la tutela dei diritti della persona.

Terzo, la portata delle risposte normative delle organizzazioni internazionali suscita l'interrogativo se profili di *governance* siano prevalenti rispetto a quelli di

disciplina, secondo una linea di tendenza ravvisabile in vari settori dei rapporti internazionali [66]. Si tratta di quei settori caratterizzati dalla dinamicità dell'interazione tra esigenze pubbliche di tutela, come ambiente, salute, sostenibilità degli scambi, degli investimenti transnazionali e dell'uso del *cyberspace*, e interessi privati.

Quarto, il contributo delle imprese appare indispensabile mediante pratiche di innovazione responsabile, come raccomandato in particolare da OCSE e OMC, e *accountability*, seppure gli Stati abbiano la responsabilità primaria sul piano internazionale e la visione di fondo delle risposte delle organizzazioni internazionali rimanga squisitamente statocentrica.

Quinto, la diffusione dell'istituzione di *partnerships* e dell'adozione di orientamenti volti a influenzare la condotta sia di Stati sia di imprese, nella logica di stampo anche etico di "*multistakeholder engagement*", con riguardo all'applicazione dell'innovazione tecnologica potenzialmente intrusiva e altresì degli algoritmi, è particolarmente significativa, in virtù dei molteplici aspetti di diversificazione e discontinuità normativa sul piano nazionale e internazionale. In effetti, l'applicazione del regime della responsabilità internazionale dello Stato, seppure riconosciuta da organizzazioni internazionali operanti nel sistema delle Nazioni Unite e da buona parte della dottrina, quale parametro normativo di riferimento prioritario sul piano internazionale nell'eventualità di illeciti internazionali nel *cyberspace*, può non essere applicabile in diverse situazioni concrete e la valorizzazione delle numerose norme internazionali non vincolanti in chiave di *governance* risulta così opportuna.

[66] Cfr. M. ARCARI, *New Technologies in International (and European) Law – Contemporary Challenges and Returning Issues*, in E. CARPANELLI, N. LAZZERINI (eds.), *Use and Misuse of New Technologies,* Springer Nature, Cham, 2019, p. 355 ss.; D. BURCHARDT, *Does Digitalization Change International Law Structurally?*, in *German Law Journal*, 2023, p. 438 ss.