Cyberspazio, troppe aree grigie: l'Italia spinge su un upgrade delle norme internazionali

Nel cyberspazio quale legge si applica? E come può uno Stati difendersi, o reagire, di fronte a un cyberattacco? Il **dibattito** per stabilire le regole del mondo cibernetico è tutto aperto. **L'Italia dà il suo contributo con un nuovo position paper** (**SCARICABILE QUI**) inviato dal ministero degli Affari esteri alle Nazioni Unite in cui **si sottolinea il valore della legge internazionale, ma si portano anche all'attenzione alcune aree grigie** su cui occorre trovare un'interpretazione o applicazione univoca della legge.

Uno dei nodi essenziali è rappresentato dalle **possibili violazioni del principio di non intervento nel cyberspazio.** Questo è particolarmente vero nel caso di **attività volte a influenzare le politiche di uno Stato, come la sua capacità di salvaguardare la salute pubblica in**

caso di una pandemia, o a manipolare le intenzioni di voto.

Protezione della **sovranità nel cyberspazio** e violazioni del principio di non intervento; applicazione della legge sulla responsabilità internazionale degli Stati alle attività svolte nel cyberspazio; cyber-operazioni e uso della forza; applicazione della legge internazionale sui **diritti umani**; **ruolo degli stakeholder privati**; cooperazione internazionale nel cyberspazio, sono i temi affrontati nel paper su "applicabilità del diritto internazionale allo spazio cibernetico: contributo a dibattito multilaterale per stabilità e sicurezza internazionali".

La sovranità nel cyberspazio e il principio di non intervento

La legge internazionale, si legge nel documento, è ritenuta dal nostro Paese "applicabile al cyberspazio" e "strumento fondamentale per assicurare un comportamento responsabile nel cyberspazio". Ciò è in linea col supporto dato dall'Italia al valore della legge sia su scala nazionale che internazionale e alla fiducia del nostro Paese nell'ordine e nella cooperazione internazionale basati sulle regole.

Tuttavia occorre continuare la discussione su alcuni punti, perché l'Italia non ha dubbi sul fatto che la legge internazionale si applichi al cyberspazio ma **"è consapevole che il modo in cui si applicano le regole e i principi attuali della legge internazionale dà luogo a significative difficoltà** inerenti alle caratteristiche tecniche del cyberspazio".

L'Italia, per esempio, attribuisce importanza fondamentale all'applicazione del **principio di sovranità nel cyberspazio, incluse le regole ancillari, come il diritto all'auto-determinazione.**

Nel caso dell'uso della forza, l'Italia sottolinea le

limitazioni della International humanitarian law, che si applica alla condotta dei belligeranti con effetti negativi sui civili in un conflitto armato, e afferma che riconoscerne l'applicabilità al cyberspazio non significa incoraggiare o permettere l'uso della forza come strumento di aggressione o risoluzione delle dispute internazionali.

Le attribuzioni di responsabilità e la difesa dei diritti umani

Di chi è la responsabilità di una violazione nel cyberspazio? **La pervasività delle tecnologie non sempre rende facile o possibile risalire agli attori di una cyber operazione che viola le regole** internazionali. Questo è un altro ambito in cui l'Italia invita ad approfondire il dibattito. Il nostro Paese riconosce l'applicabilità della legge come codificata dagli Arsiwa, gli articoli dell'International law commission sulla responsabilità degli Stati per azioni illegittime internazionali. Ma il cyberspazio ha caratteristiche peculiari che rendono difficile, nel concreto, applicare queste norme.

Oltre all'attribuzione delle responsabilità, il position paper passa in rassegna **l'aspetto della due diligence**, che richiede agli Stati di adottare tutte le misure ragionevoli sulle attività nel cyberspazio che ricadono nella loro giurisdizione al fine di prevenire, eliminare o mitigare possibili ricadute sugli interessi legittimi di un altro Stato o della comunità internazionale. Per l'Italia l'obbligo di due diligence **deve includere, tra l'altro, la difesa dei diritti umani e della pace e della sicurezza internazionale.**

Di conseguenza, gli Stati hanno l'obbligo di **non consentire che il loro territorio o le loro infrastrutture Ict siano usate per condurre attività cybercriminali** da parte di attori governativi o non governativi.

Il position paper affronta infine la questione delle

contromisure in caso di cyberattacco. Il diritto all'auto-difesa è inviolabile, ma l'adozione di contromisure adeguate all'attacco cibernetico è resa complicata, tra l'altro dalla difficoltà nel tracciamento, nella valutazione della violazione e nella stima del danno subito.

In ogni caso le contromisure non devono arrivare alla minaccia o all'uso della forza e devono restare coerenti con le norme vigenti e il rispetto dei diritti umani.

Il ruolo degli attori privati nel cyberspazio

Dato il ruolo fondamentale del settore privato nel cyberspazio, l'Italia considera la cooperazione pubblico-privata essenziale per garantire la cybersicurezza e la costruzione di infrastrutture e strumenti adatti a gestire e difendere il cyberspazio.

Le attività del cyberspazio possono anche danneggiare gli attori privati, sia singolarmente che come parte di un'alleanza con lo Stato per la costruzione e la gestione delle infrastrutture Ict.

L'Italia riconosce anche le responsabilità del settore privato per quel che riguarda i diritti umani nel cyberspazio, in linea con i principi guida dell'Onu su business e diritti umani.