

Nuova convenzione ONU sui crimini informatici: “un assegno in bianco per gli abusi di sorveglianza”

Le Nazioni Unite sono in procinto di dare vita ad un Trattato internazionale sulla lotta contro l'uso delle tecnologie dell'informazione e della comunicazione a fini criminali. In discussione dal 2021, la convenzione vuole costituire un testo di riferimento globale per la lotta all'uso **dell'informazione e delle tecnologie di comunicazione** a fini criminali. Il testo è stato elaborato da un comitato istituito ad hoc, che aveva il compito di stabilire un quadro giuridico completo contro i reati informatici. Questo è però contestato da molte associazioni, che ritengono che i suoi termini siano troppo generali e non circoscritti. Esse fanno inoltre notare come la **Convenzione di Budapest**, tutt'ora in vigore, costituisca già un quadro legislativo consolidato a livello internazionale per la lotta al cybercrimine. Le organizzazioni denunciano quindi come il Trattato costituisca un potenziale mezzo, per gli Stati, per **reprimere il dissenso** e violare i diritti umani dei cittadini.

Dopo anni di confronti, le Nazioni Unite sono riuscite a trovare un compromesso sulla stesura della Convenzione sulla cybersicurezza. Dal 29 luglio al 9 agosto scorso, a New York, si è tenuta la sessione conclusiva di discussioni sul Trattato internazionale sulla lotta contro l'uso delle tecnologie dell'informazione e della comunicazione a fini criminali, in discussione dal 2021, che intende fornire un quadro legislativo omogeneo a livello mondiale. Il testo è stato elaborato da un comitato istituito appositamente al fine di stabilire un quadro giuridico completo contro i reati informatici. L'obiettivo è quello di consolidare e intensificare la cooperazione internazionale, con un focus particolare sulla pornografia infantile online e il riciclaggio di denaro. L'adozione della Convenzione è stata accolta dagli applausi della commissione preposta e deve ora essere sottoposta all'Assemblea generale per l'adozione formale. Meno contente sono le Big Tech, le quali subiranno maggiori ingerenze da parte dei governi, ma anche i difensori dei diritti umani, che temono **una legittimazione della sorveglianza su scala globale**. «La convenzione sui crimini informatici dell'ONU è un assegno in bianco per gli abusi di sorveglianza», ha [denunciato](#) Katitza Rodriguez, policy director della privacy globale della Electronic Frontier Foundation's (EFF's). L'azienda ha chiesto ai delegati degli Stati dell'Unione Europea e alla Commissione UE di rivedere e correggere i numerosi difetti contenuti nella bozza, tra i quali vi sarebbe l'ambito di applicazione troppo ampio, che potrebbe garantire poteri di sorveglianza intrusivi senza garanzie per i diritti umani e la protezione dei dati.

La Convenzione di Budapest

«È estremamente preoccupante che ci sia un aumento globale nell'uso e **nell'abuso di strumenti e legislazioni** sulla criminalità informatica da parte di alcuni governi, che citano preoccupazioni per la sicurezza nazionale, il mantenimento dell'ordine sociale e la lotta al terrorismo, al fine di limitare la privacy, la libertà di espressione, di riunione e di

Nuova convenzione ONU sui crimini informatici: “un assegno in bianco per gli abusi di sorveglianza”

associazione e di prendere di mira e sorvegliare individui e gruppi», denuncia il [CyberPeace Institute](#) nel suo [documento](#) di critica alla Convenzione delle Nazioni Unite. «La Convenzione dovrebbe utilizzare i termini “sistema informatico” e “dati informatici” anziché proporre termini nuovi o troppo ampi che possono introdurre incertezza nell’ambito dei termini definiti e ostacolare la cooperazione internazionale. Oltre 120 Paesi utilizzano già questi termini come definiti nella Convenzione di Budapest», prosegue l’ONG, che si occupa di sicurezza informatica, rilevamento e analisi delle minacce, in sostegno di un cyberspazio sicuro e protetto. Infatti, la [Convezione di Budapest, adottata nel 2001](#), armonizza già gli elementi di diritto penale sostanziale nazionale relativi ai reati di cyber-criminalità, fornendo i poteri procedurali necessari per indagare e perseguire tali reati in un regime di cooperazione internazionale rapido ed efficace. All’interno dell’ampia gamma dei reati che la Convezione del 2001 intende colpire, i principali sono l’accesso illecito, l’interferenza di dati, le frodi informatiche, la pedopornografia e le violazioni dei diritti d’autore. Non è chiaro, dunque, perché vi sia bisogno di un nuovo trattato dai termini ampi e generali, se non per soddisfare la necessità degli Stati di operare un più ampio potere di censura e di intervento, con la conseguente possibile violazione dei diritti umani dei cittadini.

I rischi per i diritti dei cittadini

Anche Human Rights Watch ha redatto un [documento](#) di critica rispetto alla Convenzione. Secondo l’ONG, il testo del documento è viziato per via «della sua **portata mal definita ed estremamente ampia** e della sua mancanza di adeguate tutele dei diritti umani». Come spiega Human Rights Watch, il trattato non riguarda affatto la criminalità informatica, ma richiede agli Stati di stabilire **ampi poteri di sorveglianza elettronica** per indagare e cooperare su un’ampia gamma di crimini, anche reati nei quali non è coinvolto nessun sistema di informazione e comunicazione (ICT). Anche le Big Tech saranno toccate da questo nuovo quadro giuridico e saranno quindi costrette ad una maggiore censura – più di quella che già viene imposta dalle medesime – per non finire nel mirino della magistratura degli Stati nazionali. «Con maggiori poteri di sorveglianza dovrebbero derivare garanzie più solide sui diritti umani per la protezione dagli abusi. Tuttavia, questo non potrebbe essere più lontano dal caso del trattato sulla criminalità informatica delle Nazioni Unite. Rev. 3 continua a fare riferimento al diritto interno per garantire la tutela dei diritti umani e non riesce ad enumerare gli standard fondamentali in materia di diritti umani», sostiene il documento redatto da Human Rights Watch. La famosa organizzazione dei diritti umani prosegue poi in maniera molto esplicita: «La bozza di trattato delle Nazioni Unite sulla criminalità informatica somiglia a un **trattato di sorveglianza globale** per affrontare tutti i crimini, pronto a facilitare le violazioni transnazionali dei diritti umani, e supera di gran lunga l’interpretazione più espansiva possibile del mandato del Comitato ad hoc».

Nuova convenzione ONU sui crimini informatici: “un assegno in bianco per gli abusi di sorveglianza”

Le critiche dall'ONU

Anche l'Alto Commissario delle Nazioni Unite per i diritti umani (OHCHR) ha reso pubbliche le proprie perplessità e critiche nei confronti del trattato. In un documento questi [scrive](#) infatti che «La bozza riveduta contiene alcuni miglioramenti graditi. Tuttavia, l'OHCHR resta preoccupato per le **carenze significative**, poiché molte disposizioni non riescono a soddisfare gli standard internazionali sui diritti umani. Queste carenze sono particolarmente problematiche alla luce del già ampio utilizzo delle leggi esistenti sulla criminalità informatica in alcune giurisdizioni per limitare indebitamente la libertà di espressione, prendere di mira le voci dissenzianti e interferire arbitrariamente con la privacy e l'anonimato delle comunicazioni».

Le preoccupazioni più evidenti sono quindi riferite alla **libertà di espressione e di manifestazione del pensiero**, andando a ledere i diritti umani di ogni cittadino e impedendo una corretta, ampia e diversificata informazione. Se questo vale per ogni singolo cittadino in quanto tale, lo è ancor più per giornalisti e analisti, il cui lavoro sarebbe sempre passibile di censura, quando non di vera e propria criminalizzazione, secondo la volontà degli apparati statali, legittimati da un quadro normativo volutamente lasciato ampio che non specifica e rende chiari i casi di applicazione e non rende trasparenti i dispositivi con cui si proteggerebbero i diritti umani.

[di Michele Manfrin]