Cybercrime, procede l’iter della Convenzione ONU



Le ramificazioni del crimine informatico e i loro effetti su persone ed economie non sono mai apparsi così estesi. Se il 2022 si è chiuso con numerosi bilanci allarmanti circa la crescita delle minacce informatiche, è in verità da oltre un decennio che il perfezionamento delle tecnologie e la crescente diffusione di gruppi organizzati – spesso sostenuti, nonché ingentemente finanziati, da attori governativi – raccontano uno scenario di rischio sempre più complesso.

In un contesto per sua natura non limitato ai confini tradizionali, diversi Stati e organizzazioni sovranazionali (tra cui l’UE che già nel 2001 approvava la Convenzione di Budapest sulla criminalità informatica, seguita da due Protocolli addizionali) si sono dotati di apposite previsioni normative, come di specifici strumenti per la cooperazione interstatale.

Genesi ed elaborazione del documento

L’assenza di definizioni condivise e strumenti comuni a livello globale ha tuttavia frequentemente ostacolato le varie sinergie, non solo investigative o giudiziarie, essenziali per l’individuazione degli autori e per una più generale prevenzione dei reati informatici; strumenti invece previsti, per la “comune” criminalità transfrontaliera, dalla Convenzione ONU contro il crimine organizzato transnazionale (sottoscritta a Palermo nel 2000) e in parte da quella contro la corruzione del 2006, nota come Convenzione di Merida.

Superare tali difficoltà è l’obiettivo dichiarato di un testo – il primo interamente dedicato al *cybercrime* – in corso di elaborazione presso le Nazioni Unite, proprio per potenziare e

facilitare i meccanismi di monitoraggio e contrasto del fenomeno.

Un processo iniziato nel 2019, quando con la Risoluzione 74/247 l'Assemblea Generale ha istituito il Comitato *ad hoc* formato da esperti rappresentativi di tutti i Paesi membri, incaricandolo di elaborare una *"Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purpose"*; letteralmente, "Convenzione internazionale globale sul contrasto all'utilizzo di tecnologie dell'informazione e della comunicazione (ICT) per scopi criminosi".

Riunitosi per la prima volta a New York nel febbraio 2022, il Comitato *ad hoc* ha appena concluso la quarta sessione di lavori (svoltasi a Vienna fra il 9 e il 20 gennaio) e prevede di produrre una bozza da sottoporre all'Assemblea ONU entro il primo semestre del 2024.

Le riserve sui contenuti della futura Convenzione

Partendo dalla definizione dell'UNODC (UN's Office of Drugs and Crime) richiamata sin dalle prime fasi della sua elaborazione, senza dubbio la Convenzione ricomprenderà nel proprio ambito applicativo le *"cyber-dependent offences, cyber-enabled offences and, as a specific crime-type, online child sexual exploitation and abuse*".

Meno chiaro è se il documento intenderà offrire una definizione univoca dei concetti, spesso sfumati, di "attacco informatico" o di "cyber criminale"; se da un lato rinunciare alla rigidità semantica potrebbe agevolare l'attuazione della Convenzione in contesti linguistici e culturali differenti, dall'altro una certa "ambiguità" definitoria rischia però di lasciare spazio ad applicazioni arbitrarie o persino controproducenti rispetto agli scopi perseguiti.

Al riguardo diverse organizzazioni indipendenti coinvolte nel processo di stesura con un ruolo di osservazione, tra cui Privacy International e l'Electronic Frontier Foundation (EFF), hanno già espresso preoccupazione circa il potenziale impatto delle nuove regole sui diritti digitali, ricordando che la lotta contro i crimini commessi nel dominio cyber – come qualunque altra ipotesi penale – non dovrebbe mai consentire di superare i limiti imposti alle autorità a tutela della privacy individuale e di altri diritti fondamentali.

In particolare, secondo l'EFF *"the treaty, if approved, may reshape criminal laws and bolster cross-border police surveillance powers to access and share user data, implicating the privacy and human rights of billions of people worldwide".* Anche la rete sudamericana Derechos Digitales, presente alla sessione viennese, ha commentato negativamente quanto sinora emerso dai lavori del Comitato evidenziando il rischio che, se si sceglierà di rendere illecite alcune misure comunemente utilizzate a fini di anonimizzazione, offuscamento e cifratura dei dati, possano risultarne significativamente ostacolate la libertà di espressione online nonché il lavoro quotidianamente svolto in rete da attivisti, giornalisti e professionisti della cybersecurity.

Ulteriori obiezioni arrivano dagli interlocutori istituzionali: l'Unione europea ha da subito richiesto l'esclusione dal testo di ogni questione relativa alla sicurezza nazionale e alla *governance* di Internet, oltre che di eventuali obblighi imposti alle organizzazioni private tra cui i fornitori di servizi sul web, posizione condivisa da USA e UK. Richieste comprensibili in quanto relative ad aree "sensibili" della politica (come anche della politica economica) comunitaria, ma che restringono ulteriormente il potenziale campo applicativo della Convenzione.

Mentre la relazione della Cina, in direzione contraria, chiede ad esempio una maggiore pervasività della regolamentazione rispetto alla catena esecutiva dei crimini informatici, al

fine di non lasciare “fuori radar” le sempre più diffuse organizzazioni che offrono servizi di *cybercrime-as-a-service* (CaaS).

Avendo presenti tali molteplicità di approcci e prospettive, il lavoro del Comitato *ad hoc* appare tutto fuorché semplice: saranno le prossime sessioni – rispettivamente previste ad aprile e ad agosto 2023 – a fornire maggiori elementi circa la direzione della futura Convenzione ONU sul cybercrime.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/cybercrime-procede-liter-della-convenzione-onu/