SISTEMA PENALE

FASCICOLO

3/2022

ISSN 2704-8098

Sistema penale (*SP*) è una rivista *online*, aggiornata quotidianamente e fascicolata mensilmente, ad accesso libero, pubblicata dal 18 novembre 2019.
La *Rivista*, realizzata con la collaborazione scientifica dell'Università degli Studi di Milano e dell'Università Bocconi di Milano, è edita da Progetto giustizia penale, associazione senza fine di lucro con sede presso il Dipartimento di Scienze Giuridiche "C. Beccaria" dell'Università degli Studi di Milano, dove pure hanno sede la direzione e la redazione centrale. Tutte le collaborazioni organizzative ed editoriali sono a titolo gratuito e agli autori non sono imposti costi di elaborazione e pubblicazione.
La *Rivista* si uniforma agli standard internazionali definiti dal *Committe on Publication Ethics* (COPE) e fa proprie le relative linee guida.

Peer review I contributi che la direzione ritiene di destinare alla sezione "*Articoli*" del fascicolo mensile sono inviati a un revisore, individuato secondo criteri di rotazione tra i membri del Comitato scientifico, composto da esperti esterni alla direzione e al comitato editoriale. La scelta del revisore è effettuata garantendo l'assenza di conflitti di interesse. I contributi sono inviati ai revisori in forma anonima. La direzione, tramite la redazione, comunica all'autore l'esito della valutazione, garantendo l'anonimato dei revisori. Se la valutazione è positiva, il contributo è pubblicato. Se il revisore raccomanda modifiche, il contributo è pubblicato previa revisione dell'autore, in base ai commenti ricevuti, e verifica del loro accoglimento da parte della direzione. Il contributo non è pubblicato se il revisore esprime parere negativo alla pubblicazione. La direzione si riserva la facoltà di pubblicare nella sezione "*Altri contributi*" una selezione di contributi diversi dagli articoli, non previamente sottoposti alla procedura di *peer review*. Di ciò è data notizia nella prima pagina della relativa sezione.
Di tutte le operazioni compiute nella procedura di *peer review* è conservata idonea documentazione presso la redazione.

Modalità di citazione Per la citazione dei contributi presenti nei fascicoli di *Sistema penale*, si consiglia di utilizzare la forma di seguito esemplificata: N. COGNOME, *Titolo del contributo*, in *Sist. pen.* (o *SP*), 1/2022, p. 5 ss.

3/2022

LA FUTURA CONVENZIONE ONU SUL *CYBERCRIME* E IL CONTRASTO ALLE NUOVE FORME DI CRIMINALITÀ INFORMATICA

di Andrea Mattarella

Il progetto Onu sulla futura Convenzione costituisce una ulteriore tappa del processo di internazionalizzazione del contrasto penale, in una fase storica nella quale, per effetto della globalizzazione, le nuove forme di potere, attraverso gli strumenti finanziari e informatici, si liberano di ogni riferimento territoriale, spogliando il potere politico dei suoi tradizionali margini di intervento. Questa crisi del rapporto tra diritto penale, sovranità e territorio, unita alla consapevolezza che alcune categorie di reati, per la loro dimensione e per la difficoltà di accertamento, non possono essere efficacemente represse soltanto all'interno dei confini nazionali, rende indefettibile il passaggio da sistemi penali costruiti su misura dello Stato-nazione ad una dimensione internazionale del contrasto alla criminalità. La dimensione planetaria delle reti telematiche e la potenzialità di illimitata diffusione delle informazioni minacciano il principio della sovranità statale e l'esercizio stesso dei diritti fondamentali. Le organizzazioni criminali di ogni genere occupano stabilmente il cyberspazio, e si giovano della possibilità di occultarsi agevolmente. La stessa attività investigativa soffre limitazioni ed ostacoli dipendenti dai confini territoriali e dalla mancanza di uniformità delle legislazioni nazionali. Da qui l'indefettibilità di un nuovo strumento Onu sulla criminalità informatica che porti ad un'armonizzazione degli ordinamenti e garantisca il rispetto dei diritti fondamentali.

1. Introduzione.

L'Assemblea Generale delle Nazioni Unite, attraverso la Risoluzione 74/247 adottata il 27 dicembre 2019 ed intitolata "*Countering the use of information and communications technologies for criminal purposes*", ha deciso di istituire un Comitato intergovernativo di esperti (Comitato *ad hoc*), rappresentativo di tutti i paesi, per elaborare una Convenzione globale sul contrasto all'uso delle tecnologie dell'informazione e della comunicazione per scopi criminali.

Sulla base della risoluzione, il Comitato *ad hoc* ha convocato una sessione organizzativa di tre giorni nel maggio 2021, a New York, al fine di concordare il programma generale e le modalità per le sue ulteriori attività. La sessione organizzativa era originariamente prevista per il mese di agosto 2020 ma a causa dell'impatto della pandemia di COVID-19, l'Assemblea Generale, prima con la decisione 74/567 del 14 agosto 2020 e poi con la decisione 75/555 del 15 gennaio 2021, ha deliberato di rinviare la stessa sessione al 10-12 maggio 2021.

Nella predetta sessione organizzativa, il Comitato *ad hoc* ha eletto il proprio presidente – nella persona della rappresentante dell'Algeria, ambasciatrice Faouzia Boumaiza Mebarki – i vicepresidenti e il relatore, e ha discusso il programma generale e le modalità per le sue ulteriori attività. Quindi, il 26 maggio 2021, l'Assemblea Generale delle Nazioni Unite ha adottato la risoluzione 75/282, anch' essa intitolata: "Lotta all'uso delle tecnologie dell'informazione e della comunicazione a fini criminali".

Con tale risoluzione, l'Assemblea Generale ha deciso, tra l'altro, che il Comitato *ad hoc* convochi almeno sei sessioni, di 10 giorni ciascuna, seguite da una sessione conclusiva a New York, al fine di elaborare una bozza di convenzione da sottoporre all'Assemblea Generale nel corso della sua settantottesima sessione; ha inoltre deciso che il Comitato tenga la prima, terza e sesta sessione negoziale a New York e la seconda, quarta e quinta sessione a Vienna.

La prima sessione negoziale del Comitato *ad hoc* si svolgerà a New York dal 28 febbraio all'11 marzo 2022, e sarà preceduta da un incontro organizzativo che avrà luogo nella stessa sede il 24 febbraio.

Nella fase attuale, gli Stati hanno espresso le loro posizioni presentando una serie di proposte.

Il progetto Onu sulla futura Convenzione costituisce una ulteriore, importantissima tappa del progressivo processo di internazionalizzazione del diritto e della procedura penale, in una fase storica nella quale, per effetto della globalizzazione, le nuove forme di potere, attraverso gli strumenti finanziari e informatici, si liberano di ogni riferimento territoriale, spogliando sostanzialmente il potere politico dei suoi tradizionali margini di intervento[1].

In un contesto nel quale la globalizzazione ha condotto ad un crescente «divorzio tra la politica e il potere», con l'affermazione di una molteplicità di poteri di fatto, sia leciti sia illeciti, occorre ripensare su nuove basi il fondamento democratico del sistema penale[2].

Questa crisi del rapporto tra diritto penale, sovranità e territorio[3], unita alla consapevolezza che alcune categorie di reati, per la loro dimensione e per la difficoltà di

---

[1] Una trattazione generale sul tema si deve a C. PONTI, *Crimini transnazionali e diritto internazionale*, Giuffrè, Milano, 2011.

[2] Z. BAUMAN, intervista in *Il Messaggero*, 10 settembre 2012, che individua la ragione della crisi della democrazia e delle istituzioni nel divorzio tra la politica e il potere, in quanto, con la globalizzazione, i governi non hanno più un potere o un controllo dei loro paesi perché il potere è ben al di là dei territori, nella finanza, nelle banche, nei media, della criminalità organizzata o nel terrorismo.

[3] In proposito cfr. A.K. SEN, *L'idea di giustizia*, Mondadori, Milano, 2009, p. 148 ss.

accertamento, non possono essere efficacemente represse soltanto all'interno dei confini nazionali, rende indefettibile il passaggio da sistemi penali costruiti su misura dello Stato-nazione ad una dimensione internazionale del contrasto alla criminalità[4].

Questa esigenza è particolarmente accentuata per il cybercrime, trattandosi di reati dematerializzati e spogliati di ogni riferimento territoriale.

2. La crescita del cybercrime e la nuova dimensione del crimine.

Negli ultimi anni è emersa una "quarta dimensione", destinata a diventare la nuova frontiera della sovranità statale dopo la terra, il mare, il cielo e lo spazio, per la quale gli Stati dovranno concorrere nel futuro. In tale contesto, l'uso di Internet e le tecnologie dell'informazione e della comunicazione (ICT - *Information and Communication Technologies*) hanno modificato le dinamiche delle relazioni internazionali. Sotto la spinta propulsiva della rivoluzione informatica, che ha aperto nuovi canali di "democratizzazione delle informazioni e dei dati", uno degli aspetti più importanti è legato all'accesso ai dati personali, per il loro valore economico e per la nuova gestione dei rapporti commerciali che ne consegue. Nell'*e-commerce*, nelle nuove tecnologie nel settore finanziario, nell'ampliamento della ricerca verso settori nuovi come quello della raccolta dei dati sensibili per l'*intelligence*, la profilazione di dati costituisce un valore crescente, su cui si costruisce la ricchezza in tutti i servizi. Sui dati si personalizza il servizio e l'offerta su ciò che serve. L'evoluzione verso un mondo sempre più digitale, attraverso lo sviluppo tecnologico, sta permettendo un processo di conservazione dei dati e delle informazioni mai visto prima. Le aziende private possiedono infatti le reti necessarie per attaccare e difendere i settori delle telecomunicazioni, dell'energia e finanziario; oltre il 90 per cento delle comunicazioni militari e di *intelligence* americane viaggiano per telecomunicazione su reti di proprietà privata. La tematica della *cybersecurity* mette quindi al centro delle relazioni internazionali l'uso della tecnologia che è la chiave di volta per comprendere come mutano gli assetti di potere alla luce dei cambiamenti socioeconomici e politici[5].

Infatti, i paesi che riusciranno a sfruttare le nuove innovazioni potranno godere di un vantaggio strategico. Peraltro, nella misura in cui è accessibile anche ad entità private e agli individui, ed è esposto ad una serie di rischi invisibili, l'ICT sottrae agli Stati il monopolio dell'uso legittimo della forza e dell'ordine internazionale. In un mondo ormai completamente globalizzato, è possibile sostenere che chi avrà l'approccio più efficace al cambiamento tecnologico dominerà il mondo[6].

---

[4] A. BALSAMO, in A. BALSAMO – A. MATTARELLA – R. TARTAGLIA, *La Convenzione di Palermo: il futuro della lotta alla criminalità organizzata transnazionale,* Giappichelli, Torino, 2020, p. 37

[5] L. PICOTTI, *Sicurezza informatica e diritto penale*, in AA.VV., *Sicurezza e diritto penale*, a cura di DONINI-PAVARINI, Bononia University Press, 2011; U. SIEBER, *Computerkriminalität*, in U. SIEBER, F. H. BRÜNER, H. SATZGER, B. VON HEINTSCHEL-HEINEGG (Hrsg), *Europäisches Strafrecht*. Baden-Baden, 2011; M. F. WEISMANN, *International Cybercrime: Recent Developments in the Law*, in R. D. CLIFFORD (ed.), *Cybercrime*, III Ed., Carolina Academic Press, 2011.

[6] L'affermazione si deve a G. GUASTELLA, *Il dominio geopolitico dello spazio cibernetico,* Edizioni ex libris,

La dimensione planetaria delle reti telematiche e la potenzialità di dare illimitata diffusione ai messaggi ed alle informazioni minaccia il principio della sovranità statale, nella sua dimensione territoriale, e l'esercizio stesso dei diritti fondamentali della persona. La comparsa di internet, all'inizio degli anni '90, venne prevalentemente accolta con grande ottimismo, poiché si pensava che la disponibilità di uno strumento comunicativo di illimitate dimensioni, accessibile a tutti e non sottoposto ad alcuna regola o controllo, potesse favorire la libertà di informazione e la diffusione delle idee. Solo gli addetti ai lavori più avveduti segnalavano il rischio che, in uno spazio privo di regole precostituite, potesse prevalere la legge del più forte. Gli spazi informatici sono stati occupati da forti monopolisti che hanno operato un intenso condizionamento dell'informazione in tutti i settori, spesso in funzione di chiari interessi di parte, producendo sistematicamente notizie distorte o false, dotate però di capacità suggestiva e destinate ad un'ampia diffusione. Si pensi poi a gravi fenomeni come "stalking", "cyberbullismo[7]", "pedopornografia online", "revenge porn", diffamazione[8], rispetto ai quali la rete si rivela veicolo di trasmissione di comportamenti violenti nei confronti di vittime incapaci di reagire e persino spinte a tragici gesti di disperazione. Ma attraverso il web ha trovato spazio anche la propaganda del fondamentalismo islamico che ha colpito l'Europa, spesso programmando e dirigendo le azioni terroristiche proprio dal web. La gravità e la crescita esponenziale di tali condotte ha imposto la previsione di specifiche figure di reato e di misure penali e amministrative.

In tale contesto, la criminalità organizzata ha saputo sfruttare le opportunità di comunicazione immediata, globale ed anonima offerte dalla rete. Le indagini più recenti rivelano che essa utilizza la rete per le operazioni di riciclaggio e di trasferimento ed occultamento dei propri proventi, oltre che per la stessa organizzazione ed esecuzione "da remoto" di operazioni illecite.

Per utilizzare un'espressione efficace, in alcune intercettazioni un boss mafioso affermava testualmente come il "clic" di un computer contasse oggi molto di più del grilletto di una pistola.

Le organizzazioni criminali di ogni genere occupano oggi stabilmente il cyberspazio, e si giovano della possibilità di occultarsi agevolmente, approfittando della sua estensione globale. La stessa attività investigativa soffre limitazioni ed ostacoli dipendenti dai confini territoriali e dalla mancanza di uniformità delle legislazioni nazionali, che gli accordi internazionali in materia finora non sono riusciti a superare. In alcuni casi le richieste di dati informativi, volte ad identificare gli autori di reati informatici, vengono bloccate dal rifiuto da parte degli Stati ove sono situate le "memorie" o persino da parte dei gestori privati, che si avvalgono di legislazioni locali particolarmente favorevoli. Paradossalmente, la stessa rete, che spesso non riesce a

---

Palermo, 2020, p. 151, cui si rinvia per una trattazione di carattere socio-politico del tema.

[7] Osservazioni utili sul contrasto al fenomeno in esame nell'ordinamento italiano sono svolte da C. PANICALI, *Il cyberbullismo: i nuovi strumenti (extrapenali) predisposti dalla legge n. 71/2017 e la tutela penale*, in *Responsabilità Civile e Previdenza*, 2017, n. 6.

[8] L. BISORI, *La diffamazione*, in CADOPPI-CANESTRARI-PAPA, *I reati contro la persona. Reati contro l'onore e la libertà individuale*, Utet, Torino, 2006.

proteggere la riservatezza delle vittime, si rivela invece efficiente nell'assicurare l'anonimato ai responsabili dei delitti.

Allo stato, non esiste una definizione normativa del crimine cibernetico[9]. In prima approssimazione, esso si distingue dalla criminalità tradizionale per l'assenza di confini fisici e geografici. Ciò disorienta le vittime rendendole più vulnerabili, per l'impossibilità di reagire, data l'incapacità di percepire l'attacco fisicamente. Dall'altro lato, il cybercriminale è agevolato dalla disponibilità diffusa di malware sulla rete, e dal fatto che il cybercrime non richiede particolari capacità tecniche.

Molti cybercriminali provengono dai paesi in via di sviluppo e non hanno un'istruzione avanzata; essi iniziano la loro carriera criminale già nell'adolescenza, spinti generalmente da motivazioni socioeconomiche. Si tratta di individui prevalentemente di sesso maschile, di età compresa tra i 18 e i 30 anni, il cui *modus operandi* consiste nel riunirsi in gruppi piccoli o medi. Dati tratti dal Report annuale di Europol del 2015 intitolato "Internet Organised Crime Threat Assessment" (IOCTA) suggeriscono che l'80% dei cybercrime necessita infatti di un'organizzazione definita. Nasce in queste circostanze il cosiddetto "crimine cibernetico organizzato". Esso si caratterizza per una maggior concentrazione nell'Est Europa, in Medio Oriente, e in Nord America, e predilige le operazioni di scambio e vendita di servizi, di consulenza, diffusione di virus, affitto di *botnet*, servizi spam, *hosting*, e le modalità di associazione ed organizzazione più disparate che vanno dall'uso di reti "underground" e parallele ad Internet, ad esempio Thor e la Darknet, o "Deep Web", alla cosiddetta "glocalization" dei gruppi, ossia l'esercizio di azioni transnazionali tendenti alla "prossimità locale e culturale".

Il mercato del crimine cibernetico, basato sostanzialmente su furti di dati ed estorsioni, ha praticamente superato il mercato della droga, ottenendo quasi il doppio dei ricavi illeciti[10].

Occorre considerare, inoltre, che gran parte delle tecnologie e delle competenze private in questo campo è di proprietà di imprese, che decidono generalmente di non denunciare gli attacchi subiti per evitare danni reputazionali o perdite in Borsa; ciò accentua la vulnerabilità del sistema.

A ciò deve aggiungersi la capacità dei terroristi di inserirsi nelle reti, pur non potendo eguagliare la capacità cibernetica di uno Stato.

I settori principali del crimine cibernetico includono il furto e la manipolazione dei dati sensibili, la contraffazione dei prodotti, il sistema delle criptovalute e il riciclaggio.

A seconda degli attori e delle finalità, il Quadro Strategico annuale per la sicurezza nello spazio cibernetico elaborato dalla Presidenza del Consiglio dei Ministri italiana nel 2013 ha distinto quattro macro-categorie:

---

[9] Per un inquadramento sistematico, L. PICOTTI, *Diritto penale e tecnologie informatiche: una visione di insieme*, in AA.VV., *Trattato di diritto penale – Cybercrime*, diretto da CADOPPI-CANESTRARI-MANNA-PAPA, Utet, 2019; V. PECORELLA, *Diritto penale dell'informatica*, Cedam, 2006; sempre V. PECORELLA, voce *Reati informatici,* in *Enc. dir., Annali,* vol. X, Giuffrè, 2017.

[10] CIS, *Italian Cyber Security Report 2015*, *Rapporto annuale sulla sicurezza*, in www.cybersecurityframework.it.

- *Cyber-crime* (criminalità cibernetica): il complesso di attività con finalità criminali che vanno dalla frode telematica al furto d'identità fino alla sottrazione indebita d'informazioni, creazioni e/o proprietà intellettuali;
- *Cyber-espionage* (spionaggio cibernetico): l'acquisizione indebita di dati e/o informazioni sensibili, proprietarie o classificate;
- *Cyber-terrorism* (terrorismo cibernetico): l'insieme delle azioni ideologicamente motivate, volte a condizionare uno Stato o un'organizzazione internazionale;
- *Cyber-warfare* (guerra cibernetica): l'insieme delle attività e delle operazioni militari pianificate e condotte allo scopo di conseguire effetti nel predetto ambiente.

Un campo da non sottovalutare è poi quello dell'*intelligence*; esso può diventare il vettore attraverso cui il cybercriminale, o l'organizzazione criminale, grazie al furto di dati, riesce ad infiltrarsi in un sistema. È dunque l'*intelligence* che prepara il terreno all'attacco che verrà condotto. Rispetto a quella del passato, inoltre, l'*intelligence* attuale dispone di più sofisticati strumenti tramite i quali poter aumentare l'asimmetricità – caratteristica saliente delle tecniche d'attacco cibernetico – e condurre più agevolmente le operazioni. Questo è un fattore che va evidenziato a causa dell'immensa quantità di dati che l'*intelligence* cibernetica può raccogliere e gestire. Se però si ha a disposizione un efficace strumento di lettura e di valutazione dei dati, unito a un chiaro obiettivo, anche la semplice raccolta dei dati aperti esistente sulla rete potrebbe essere sufficiente per penetrare segreti di Stato.

Passando agli scenari di guerra veri e propri, si è già fatto ricorso più volte, nell'arco degli anni, all'uso di attacchi cibernetici in funzione di supporto alle operazioni militari. Un ulteriore scenario da considerare è quello relativo all'uso dell'arma cibernetica in funzione strategica, non più quindi come supporto ma come arma principale di attacco contro un paese; quest'ipotesi è stata discussa anche in sede Nato quando si è sostenuto che gli attacchi cibernetici potessero fare scattare il *casus foederis* dell'Alleanza a difesa dello Stato aggredito, ai sensi dell'articolo 5 del Trattato istitutivo.

Generalmente, l'attacco cibernetico si serve di un algoritmo codificato a mezzo di un computer per diffondere degli effetti pregiudizievoli di varia natura, a seconda della tipologia di attacco o del sistema bersaglio di questo[11].

L'attacco cibernetico ricomprende una vasta gamma di tecniche. Tra gli strumenti utilizzabili, uno dei più diffusi è il *malware*, ovvero un programma avente lo scopo di cagionare danni diffusi, quali il disturbo o il malfunzionamento di una rete, la sottrazione di informazioni, l'accesso non autorizzato a reti e sistemi. Un altro tipico strumento di attacco è il DDos (*Distributed Denial of Service*), meno sofisticato del *malware*, ma non meno efficace. Per un attacco Ddos è sufficiente generare una massiccia quantità di e-mail, idonea a comportare il blocco di un sito web. A questo punto, gli obiettivi di un attacco cibernetico possono essere due: le informazioni o la provocazione di un danno fisico. Un attacco può colpire direttamente un *software* oppure può colpire l'*hardware*

[11] G. GUASTELLA, *Il dominio geopolitico dello spazio cibernetico,* cit., p. 57 ss.

attraverso il *software*. Naturalmente si può diversificare l'effetto dell'attacco a seconda che questo sia condotto contro un sistema in uso a un privato o una famiglia o sia lanciato contro computer privati in uso a dipendenti di imprese o dello Stato o, ancora, contro *mainframe* (grandi computer costituiti da una potente unità centrale di elaborazione dati alla quale sono collegati numerosi terminali) aziendali o statali. Per esempio, un attacco cibernetico può essere finalizzato a paralizzare le infrastrutture di comunicazione di un paese o la rete di trasporto ferroviaria e aerea civile, con il rischio di scontri fra treni o di disastri aerei[12].

Nel contesto globale descritto, è necessario menzionare il pericolo già rappresentato dall'Isis. I vertici del cosiddetto Stato Islamico avevano ben compreso che una guerra analoga a quella tradizionale, combattuta anche con strumenti tecnologici, avrebbe potuto portare risultati anche maggiori di quelli conseguibili con le armi militari convenzionali. Così, nel 2014, Al-Bhagdadi, soprannominato "l'informatico" dell'Isis, ideò il *Cyber Caliphate* per combattere la Cyber Jihad, facendo propria un'intuizione in passato sviluppata anche da Bin Laden. Inizialmente, il Califfato Cibernetico ha reclutato un gruppo di giovani hackers di età compresa tra i 18 e i 24 anni, istituendo delle "hackers division", basate su un organico complessivo di circa 3 mila hackers "effettivi", dislocati in ogni angolo del pianeta, inclusi gli Stati Uniti e l'Europa. L'attività dei cc.dd. cyber jihadisti consiste nella predisposizione di cyber attacchi verso tutti i paesi considerati "nemici" o "infedeli" e nell'opera di proselitismo e propaganda dello Stato Islamico. Tra gli strumenti di riferimento per le attività di proselitismo e di coordinamento delle cellule terroristiche sparse in tutto il mondo vi sono i social network, che contengono immagini e video in grado di influenzare psicologicamente le masse. A conferma di ciò, l'utilizzo dei social ha portato ad una notevole impennata del numero dei combattenti reclutati a livello mondiale. Solo in Europa, secondo una stima della CIA (*Central Intelligence Agency*) risalente al 2014, il numero degli arruolati occidentali nelle file dell'Isis sarebbe stato tra i ventimila e i venticinquemila. Foraggiate con finanziamenti pari solo a quelli dedicati all'acquisto di armi e munizioni, le hacking division del Sedicente Stato Islamico combattevano quotidianamente una guerra reale nel mondo virtuale anche per tentare di introdursi all'interno dei sistemi informatici di tutti i Paesi "nemici" allo scopo di danneggiare i sistemi o rubare i dati che vi sono conservati. Ma una parte corposa delle attività condotte del *Cyber Caliphate* ha riguardato proprio l'acquisizione di informazioni da fonti aperte soprattutto dai social network, in grado di fornire una conoscenza "individuale" e di "massa" di grande rilevanza ai fini della conduzione di azioni di persuasione, disinformazione e "intossicazione" informativa. All'interno del *Cyber Caliphate* esisteva una struttura appositamente creata per condurre attività di propaganda e comunicazione nel mondo virtuale: Al-I'tisaam Media. Nell'ambito di questa *media enterprise* operavano analisti di *intelligence*, specialisti della comunicazione, tecnici specializzati nella realizzazione e montaggio video, web

[12] Uno studio approfondito sugli effetti paralizzanti degli attacchi informatici è condotto da UNITED NATIONS HUMAN RIGHTS COUNCIL, *Ending Internet shutdowns: a path forward*, United Nations, 15 June 2021, in www.undocs.org; ancora, T. RYAN-MOSLEY, *Why you should be more concerned about internet shutdowns*, MIT Technology Review, 9 September 2021, in www.technologyreview.com.

designer, commentatori e registi. Di particolare impatto sono stati i video incessantemente prodotti e diffusi in rete nella fase di maggior virulenza dell'organizzazione, accomunati da scene raccapriccianti e di inaudita violenza.

Ciò che rende il terrorismo così difficile da combattere non è solo la sua ideologia ma anche il metodo di cui si avvale.

In definitiva, si comprende come il potere dei moderni sistemi di comunicazione abbia un ruolo determinante nelle strategie del crimine transnazionale.

Con l'entrata in vigore del Trattato di Lisbona la "criminalità informatica" è stata inserita nell'art. 83 TFUE fra i fenomeni criminosi di natura grave e transnazionale su cui l'Unione Europea ha competenza penale[13]. A livello europeo, possono citarsi alcuni interventi, come la direttiva 2011/93/UE relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e la Direttiva 2013/40/UE, relativa agli attacchi contro i sistemi di informazione.

Infine, il 14 aprile 2021, la Commissione europea ha presentato la Comunicazione relativa alla prima Strategia *ad hoc* in materia di criminalità organizzata dopo l'entrata in vigore del Trattato di Lisbona[14]. Tale Strategia si riferisce al periodo 2021-2025 e individua le linee di intervento prioritarie in tema di contrasto ai gruppi criminali, con l'obiettivo di assicurare una migliore protezione dei cittadini, dell'economia e delle istituzioni europee contro la criminalità organizzata. L'opportunità di proseguire e consolidare l'azione di contrasto intrapresa a livello europeo si giustifica soprattutto in considerazione delle modalità operative particolarmente pervasive cui i gruppi criminali ricorrono nel perseguimento dei propri interessi, dal momento che gli stessi possono avvalersi sia di strutture territoriali sia di mezzi informatici estremamente sofisticati.

La "criminalità informatica" non consiste in una categoria definita giuridicamente, anche se compare in fonti europee e sovranazionali[15].

Allo stesso modo non si rinviene una definizione internazionalmente riconosciuta di "*computer related crime*" o "*cybercrime*"[16]. Sul piano empirico, essa

---

[13] Per una recente analisi della normativa europea in materia, v. L. PICOTTI, *La nozione di "criminalità informatica" e la sua rilevanza per le competenze penali europee*, in *Riv. trim. dir. pen. ec.*, 4, 2011; sulle competenze dell'Unione, v. R. FLOR, *Le prospettive de jure condendo del c.d. data retention nel cloud scenario, tra limiti ontologici, limiti costituzionali e tutela dei diritti fondamentali*, relazione presentata al convegno "*Limiti convenzionali e costituzionali del 'Diritto Penale Europeo' dopo il Trattato di Lisbona – Il dibattito in Germania ed in Italia*", Verona, 16-17 settembre 2011.

[14] F. VILASI, *La strategia dell'Unione Europea per la lotta alla criminalità organizzata: la centralità dell'informazione e le prospettive di riforma*, in *Riv. studi e ric. sulla criminalità organizzata*, Vol. 7/ n. 2, 2021.

[15] COM(2012) 140 final.

[16] Si veda già M. BRIAT, U. SIEBER (eds.), *Computer Related Criminality: Analysis of Legal Policy in the OECD Area*, Parigi 1986. Sul piano processuale, le decisioni quadro sul mandato d'arresto europeo (2002/584/GAI) e sull'applicazione del principio del reciproco riconoscimento delle decisioni di confisca (2006/783/GAI), che includono la "criminalità informatica" nelle liste di reati per cui si prescinde, in conformità con il principio del mutuo riconoscimento, dal requisito della doppia incriminazione per l'esecuzione diretta dei provvedimenti emessi dall'autorità giudiziaria dello Stato richiedente. Vedi per tutti L. PICOTTI, *La nozione di "criminalità informatica"*, cit., pp. 827 e ss. Nella letteratura tedesca, anche sul richiamo alle fonti sovranazionali e sulle nuove competenze penali dell'Unione Europea, basti il rinvio a U. SIEBER, *Computerkriminalität*, in U. SIEBER, F.H. BRÜNER, H. SATZGER, B. VON HEINTSCHEL-HEINEGG (Hrsg), *Europäisches Strafrecht*. Baden-Baden, 2011, pp. 393 e ss.

abbraccia una molteplicità di comportamenti lesivi di interessi penalmente rilevanti, riconducibili ai "reati informatici", introdotti in molti ordinamenti nazionali. Dopo l'"esplosione" di Internet, si è assistito al passaggio dalla dimensione "privata" o "individuale" del computer e delle delimitate reti di computer alla dimensione "pubblica" o "collettiva" dei sistemi, basati sull'interconnettività globale. Nell'attuale società dell'informazione la "criminalità informatica" risulta essere dunque flessibile e mutevole. Sul piano del diritto penale sostanziale, la "criminalità informatica" può includere sia fattispecie legali costruite, sul piano della formulazione, con elementi di tipizzazione connessi a procedimenti di automatizzazione di dati o informazioni, ovvero legate a modalità, oggetti o attività di carattere tecnologico (reati informatici in senso stretto)[17], sia tutte quelle fattispecie incriminatrici "comuni" che, pur non presentando espressamente elementi tipici caratterizzati dalla tecnologia, possono essere applicate a fatti commessi tramite la tecnologia, la rete o nel cyberspace[18] (reati informatici in senso lato).

In questo contesto assume rilevanza anche la distinzione fra reati cibernetici in senso stretto e reati cibernetici in senso lato. Nei primi l'elemento tecnologico e specializzante è caratterizzato proprio dalla connessione in rete o dalla fruibilità del cyberspace[19]. I secondi, invece, presentano modalità o possibilità di realizzazione concreta "in rete" e sono formulati in termini più generali ed elastici, tanto da essere realizzabili o concepibili a prescindere dall'informatica e dalla rete[20].

Questa impostazione teorica trova un riscontro nelle disposizioni di carattere processuale previste dalla Convenzione sulla criminalità informatica del Consiglio d'Europa (Convenzione di Budapest), che si applicano non solo ai reati da essa previsti (artt. 2-11), ma anche a tutti gli illeciti commessi attraverso i sistemi informatici ed a quelli per il cui accertamento è necessaria la raccolta della prova elettronica (ex art. 14).

Una parte della dottrina americana ritiene che la categoria "cybercrime" comprenda almeno tre sub-categorie: reati in cui il computer o il sistema informatico

---

[17] Vedi M.F. WEISMANN, *International Cybercrime: Recent Developments in the Law*, in R.D. CLIFFORD (ed.), *Cybercrime*, III Ed., Carolina Academic Press, 2011, 257, p. 258.

[18] Si pensi, nell'ordinamento italiano, all'accesso abusivo a sistemi informatici (art. 615 ter c.p.) o alla frode informatica (art. 640 ter c.p.). Questa categoria di reati informatici si connota per un nuovo oggetto passivo su cui la condotta va a cadere (quali i dati, le informazioni, i programmi od altri "prodotti" informatici o digitali, compresi i "sistemi informatici" in genere) oppure dal fatto che il computer ed i prodotti informatici in genere costituiscono lo strumento tipico di realizzazione del 'fatto' criminoso. Così L. PICOTTI, *La nozione di "criminalità informatica"*, cit.

[19] Si consideri, nel sistema italiano, la truffa comune (art. 640 c.p.), che può essere commessa attraverso l'invio di e-mail ingannevoli che inducono in errore il destinatario determinandolo ad effettuare un atto di disposizione patrimoniale su conti correnti online. Oppure si pensi alla diffamazione online, o alle forme di manifestazione o diffusione del pensiero o di contenuti illeciti, quale la rivelazione od agevolazione "in qualsiasi modo" della conoscenza, da parte di terzi non legittimati, di una notizia che debba rimanere segreta. Su tali categorie si veda L. PICOTTI, *Biens juridiques protégés et techniques de formulation des incriminations en droit pénal de l'informatique*, in *Rev. Int. Droit pénal*, 2006, n. 3/4, pp. 525 ss.

[20] Si pensi, ad esempio, agli artt. 171, lett. a) bis e 171 ter, co. 2, lett. a) bis della l. n. 633/41 (che sanzionano la diffusione abusiva tramite l'immissione in un sistema di reti telematiche di un'opera dell'ingegno protetta). Su tali reati si consenta di rinviare a R. FLOR, *Tutela penale e autotutela tecnologica,* cit., pp. 329 e ss.

costituiscono l'obiettivo delle attività criminali; reati in cui il computer e, in generale, le nuove tecnologie ed Internet, rappresentano gli strumenti per commettere o preparare un reato; reati in cui il sistema informatico e la rete costituiscono solo un "aspetto incidentale" nella commissione dell'illecito[21].

3. La Convenzione di Budapest e il ruolo "suppletivo" della Convenzione di Palermo.

La Convenzione di Budapest sulla criminalità informatica, firmata il 23 novembre 2001 nell'ambito del Consiglio d'Europa, è il primo accordo internazionale riguardante i crimini commessi attraverso internet o altre reti informatiche, con l'obiettivo di realizzare una politica comune fra gli Stati membri, attraverso l'adozione di una legislazione appropriata, che consenta di combattere il crimine informatico in maniera coordinata.

Essa è stata ratificata dall'ordinamento italiano nel 2008 e mira principalmente ad armonizzare i sistemi penali nazionali e le disposizioni connesse nel settore della criminalità informatica, prevedendo altresì i necessari strumenti per l'indagine e il perseguimento di tali reati compresa la cooperazione internazionale. Gli Stati hanno preso atto che la rivoluzione nelle tecnologie dell'informazione ha cambiato radicalmente la società e pervaso quasi ogni aspetto delle attività umane[22].

La Convenzione di Budapest si basa quindi sulla consapevolezza che le nuove tecnologie mettono in discussione i concetti legali esistenti. Le informazioni e le comunicazioni fluiscono più facilmente in tutto il mondo e i criminali riescono ad agire localizzati in luoghi diversi da quelli in cui i loro atti producono i loro effetti. Di fronte a questo, le leggi nazionali, tradizionalmente limitate a un territorio specifico, non sono sufficienti. Pertanto, gli Stati hanno preso consapevolezza che le soluzioni alle problematiche descritte devono essere rintracciate nel diritto internazionale, sempre nel rispetto dei diritti umani.

Sul versante sostanziale[23], la Convenzione richiede che siano incriminate le fattispecie di accesso illecito, intercettazione illecita, interferenza di dati, interferenza in

---

[21] Vedi S. BRENNER, *Defining Cybercrime: A Review of Federal and State Law*, in R. D. Clifford (ed.), *Cybercrime*, cit., 15-104, 17, cui l'Autrice si chiede se la categoria "*cybercrime*" abbracci nuove forme di criminalità e di crimini, ovvero se non si tratti piuttosto di "vecchio vino in nuove bottiglie" ("*old wine in new bottles*"). In verità questa espressione non è così distante da quella utilizzata da BARLOW - "*Selling wine without bottles*" - con la quale rappresenta il nuovo scenario dominato dalla tecnologia, che ha determinato la trasformazione dell'architettura tipica su cui poggiava la tutela del diritto d'autore, e la crisi del sistema di tutela della proprietà intellettuale, dovuta alla proliferazione sia di fenomeni criminosi nuovi, che di "vecchi" fenomeni realizzati con nuovi strumenti. Vedi J.P. BARLOW, *Selling Wine without Bottles*: *The Economy of Mind on the Global Net*, in P. LUDLOW (ed.), *High Noon on the Electronic Frontier, Conceptual Issues in Cyberspace*, III ed., MIT, 1999, pp. 9 e ss., citato da R. FLOR, *Tutela penale e autotutela tecnologica,* cit., p. 250.

[22] Sui profili relativi alla ratifica della Convenzione, v. PICOTTI, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale,* in *Dir. pen. proc.*, n.6/2008.

[23] L. PICOTTI, *Ratifica della Convenzione Cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo,* in *Dir. Internet,* 2008, p. 5443.

un sistema, uso improprio di dispositivi, falsità informatica, frode informatica, pedopornografia e reati in materia di diritto d'autore.

Lo scopo della Sezione 1 della Convenzione (articoli 2 – 13) è prevenire e reprimere la criminalità informatica, stabilendo uno standard minimo comune per i reati inclusi nell'elenco, che può essere esteso dal diritto interno. La sezione è suddivisa in cinque titoli.

Il titolo I comprende il nucleo essenziale dei reati informatici, e cioè i reati contro la riservatezza, l'integrità e la disponibilità dei dati e dei sistemi informatici. Il titolo descrive la tipologia dei reati contemplati, ovvero l'accesso non autorizzato e la manomissione illecita di sistemi, programmi o dati.

I titoli II, III e IV includono altri tipi di "reati informatici", che svolgono un ruolo maggiore nella pratica e in cui i sistemi informatici e di telecomunicazione sono utilizzati come mezzo per attaccare determinati interessi che per lo più sono già protetti dal diritto penale contro gli attacchi che utilizzano mezzi tradizionali.

I reati del Titolo II (frode e falsità informatica) sono stati aggiunti seguendo i suggerimenti delle linee guida della Raccomandazione n. R (89) 9 del Consiglio d'Europa.

Il Titolo III riguarda i "reati di contenuto di produzione o distribuzione illecita di pedopornografia mediante l'uso di sistemi informatici" considerati come uno dei *modi operandi* della criminalità più pericolosi degli ultimi anni.

Il comitato che ha redatto la Convenzione ha discusso la possibilità di includere altre fattispecie, come la diffusione di propaganda razzista attraverso i sistemi informatici. Tuttavia, il comitato non è stato in grado di raggiungere un consenso sulla criminalizzazione di tale condotta, in quanto, nonostante un notevole sostegno a favore della sua inclusione come reato, alcune delegazioni hanno addotto, pretestuosamente, in senso contrario all'inclusione di tale disposizione motivi di libertà di espressione. Rilevando la complessità della questione, si è deciso che la commissione deferisse al Comitato europeo sui problemi della criminalità (CDPC) la questione dell'elaborazione di un Protocollo aggiuntivo alla Convenzione.

Il titolo IV della Convenzione prevede i "reati connessi alla violazione del diritto d'autore e dei diritti connessi". Si tratta di una delle forme più diffuse di criminalità informatica.

Il Titolo V, infine, contiene ulteriori disposizioni in materia di tentativo, favoreggiamento, sanzioni e misure sulla responsabilità degli enti[24].

Giova sottolineare che sebbene le disposizioni di diritto sostanziale si riferiscano a reati che utilizzano la tecnologia dell'informazione, la Convenzione utilizza un linguaggio tecnologicamente neutrale al fine di garantire che le fattispecie ivi previste possano essere applicate alle tecnologie attuali e a quelle utilizzate in futuro.

Una specificità dei reati contemplati è l'espresso requisito che le condotte in questione siano poste in essere "senza diritto" e cioè abusivamente, nella forma di una

[24] Per un inquadramento della responsabilità degli enti, S. BELTRANI, *Reati informatici e D.lgs. 231/2001 alla luce della legge di attuazione della Convenzione di Budapest*, in *Resp. amm. soc. ed enti*, 2008, n. 4; ancora, A. GULLO, *I reati informatici*, in *Responsabilità da reato degli enti*, Giappichelli, Torino, 2021.

clausola di illiceità speciale, che postula la violazione di norme extrapenali. In altri termini, le condotte descritte non sono sempre punibili di per sé, ma possono essere lecite o giustificate non solo nei casi in cui sono applicabili le classiche scriminanti, ma anche laddove altri principi o interessi portano all'esclusione di responsabilità penale. La Convenzione, quindi, non colpisce quelle attività intraprese in esecuzione di ordini legittimi dell'autorità, ad esempio per mantenere l'ordine pubblico, proteggere la sicurezza nazionale o indagare sui reati. Inoltre, la Convenzione esclude le attività legittime e inerenti alla progettazione ed alla messa in sicurezza delle reti. Spetta agli Stati parte determinare come tali esenzioni debbano operare all'interno dei sistemi giuridici nazionali.

In relazione all'elemento soggettivo, ai fini della responsabilità, tutti i reati contenuti nella Convenzione devono essere commessi "intenzionalmente", e in taluni casi si richiede l'ulteriore elemento del dolo specifico, come avviene nell'articolo 8 sulle frodi informatiche, con la previsione dell'intento di procurare un vantaggio economico.

La sezione di diritto processuale, che si applica a qualsiasi reato commesso a mezzo di un sistema informatico o la cui prova può essere fornita in forma elettronica, determina le garanzie comuni e stabilisce alcuni strumenti procedurali, come la conservazione celere dei dati archiviati e di traffico, gli ordini di produzione, la perquisizione e sequestro di dati informatici, la raccolta in tempo reale dei dati sul traffico e l'intercettazione di dati di contenuto.

Il capo II si chiude con le disposizioni sulla giurisdizione, mentre il capo III contiene le disposizioni in materia di assistenza giudiziaria e di criminalità informatica nonché le norme in materia di estradizione. Si prevede che quando non esiste una disciplina giuridica specifica, un trattato o una convenzione tra le parti, si applicano le disposizioni della Convenzione, mentre, laddove nell'ordinamento nazionale esista una normativa in materia, le disposizioni esistenti si applicano anche all'assistenza.

Nel novembre 2021, in occasione del XX anniversario della Convenzione di Budapest contro il crimine informatico, ed in concomitanza con il passaggio di consegne per la Presidenza del Consiglio d'Europa dall'Ungheria all'Italia, il Comitato dei Ministri del Consiglio d'Europa ha adottato il secondo Protocollo addizionale contro il crimine informatico, relativo alla cooperazione rafforzata ed alla divulgazione delle prove elettroniche.

Il Protocollo ha l'obiettivo di fornire "*a legal basis*" per una mutua assistenza tra le autorità pubbliche dei diversi Stati e i fornitori dei servizi on-line, per rafforzare la cooperazione e la divulgazione delle prove elettroniche, nonché fornire garanzie per la protezione dei dati personali.

A fonte della proliferazione della criminalità informatica e della crescente complessità di ottenere prove elettroniche che possono essere archiviate in giurisdizioni straniere, multiple, mutevoli o sconosciute, i poteri delle forze dell'ordine sono limitati dai confini territoriali. Allo stato attuale, il perseguimento dei crimini informatici è ostacolato nel reperimento delle prove nel mondo virtuale[25]. Ciò è dovuto in particolare

[25] Per una trattazione generale delle indagini sui crimini informatici, v. S. ATERNO, *Digital forensics*

alla dialettica tra territorialità della giurisdizione e de materializzazione della rete. Di conseguenza, solo una piccola parte dei crimini informatici segnalati alle autorità di giustizia penale porta a decisioni giudiziarie. In risposta a tale problematica, il secondo Protocollo fornisce una base giuridica per la divulgazione delle informazioni sulla registrazione dei nomi di dominio e per la cooperazione diretta con i fornitori di servizi per le informazioni sugli abbonati, mezzi efficaci per ottenere informazioni sugli abbonati e dati sul traffico, cooperazione immediata in caso di emergenza, strumenti di mutua assistenza, nonché garanzie per la protezione dei dati personali. Il testo dovrebbe essere aperto alla firma nel maggio 2022.

La Convenzione di Budapest, per numerosi ordinamenti tra cui quello italiano, ha rappresentato una prima base per l'implementazione del contrasto al cybercrime, sulla base di alcuni caratteri comuni.

Tuttavia, nonostante la Convenzione abbia prodotto molteplici risultati positivi, solo 66 Stati hanno proceduto alla ratifica: è un numero notevolmente superiore a quello degli Stati membri del Consiglio d'Europa, ma assai inferiore a quello dei membri delle Nazioni Unite.

Per tale ragione, un ruolo "suppletivo" di rilevanza fondamentale è stato svolto dalla Convenzione Onu contro il crimine organizzato transnazionale, firmata a Palermo nel 2000. Quest'ultima costituisce il principale strumento internazionale di riferimento contro tutte le forme di criminalità, in quanto vede la partecipazione di oltre 190 Stati e contiene soprattutto norme innovative in materia di indagini, sorveglianza elettronica, cooperazione giudiziaria e responsabilità da reato degli enti, ivi compresi gli intermediari di internet.

Inoltre, essa si caratterizza per una nozione ampia di reato grave di dimensione transnazionale e di gruppo organizzato.

La tipizzazione della nozione di "gruppo criminale organizzato" risente della "*vocazione universale*" di tale disciplina, per la necessità di formulare una definizione di criminalità organizzata che fosse suscettibile di essere recepita dai singoli Stati nazionali[26] e che risultasse idonea a fotografare un fenomeno mutevole, quello del crimine organizzato transnazionale.

D'altronde, come è stato condivisibilmente affermato, "*la creazione di una precisa tassonomia della criminalità organizzata è un compito assai difficile, per non dire impossibile, tali*

(investigazioni informatiche), in *Digesto delle discipline penalistiche,* Aggiornamento, VIII, Utet, Torino, 2014.

[26] "*Le difficoltà sono d'altronde note a chi su scala geografica ben più limitata prova da tempo ad approntare risposte comuni al fenomeno della criminalità organizzata: persino in un ambito culturalmente abbastanza omogeneo come l'Unione Europea (anche se con i recenti allargamenti l'affermazione è un po' meno vera di prima) le disomogeneità ordinamentali rendono faticoso il cammino verso l'adozione di standards comuni di incriminazione per la partecipazione ad una organizzazione criminale e l'implementazione dei correlati strumenti processuali e di cooperazione giudiziaria*": così S. FIORE, *La partecipazione al gruppo criminale organizzato*, in E. ROSI (a cura di), *Criminalità organizzata transnazionale e sistema penale italiano, La Convenzione ONU di Palermo*, Milano, 2007, p. 108. Sul tema, cfr. l'accurato contributo di V. MILITELLO, *Criminalità organizzata transnazionale ed intervento europeo fra contesto e garanzie*, in *Rivista trimestrale di diritto penale dell'economia*, 2011, fasc. 4, pp. 811-826.

sono la varietà, le sfumature e la flessibilità del fenomeno che persino le più aggiornate proposte di classificazione rischiano di non essere sufficientemente descrittive o esaustive"[27].

Questa "*notevole ampiezza e flessibilità*"[28], che caratterizza la Convenzione di Palermo, ha consentito di includere negli anni anche le emergenti forme di criminalità informatica, supplendo alla limitata adesione ricevuta dalla Convenzione di Budapest contro il cybercrime.

Un altro aspetto particolarmente significativo della Convenzione di Palermo che può rilevare nel contrasto ai reati informatici è la previsione (analoga a quella della Convenzione di Budapest) relativa alla responsabilità delle persone giuridiche e in particolare dei soggetti che, a vario titolo, operano nel complesso universo di internet[29].

I reati commessi online sono proprio tra le forme di criminalità transnazionale più frequenti, e, in molti paesi, i servizi offerti dagli intermediari di internet sono tra i più rilevanti economicamente. Può anzi dirsi, per le ragioni esposte, che i cybercrimes siano i reati transnazionali per eccellenza.

La categoria degli intermediari di internet è vastissima: essa comprende i motori di ricerca, gli *internet access provider*, che offrono l'accesso alla rete, gli *online payments provider* che consentono di effettuare i pagamenti online, i *domain name registrar*, dai quali si affittano i domini web, le società di *web hosting* che ospitano i siti web, le reti pubblicitarie online.

Nell'ambito dell'attività di implementazione della Convenzione di Palermo, si riscontra un crescente interesse per l'applicazione alle molteplici figure di intermediari di internet della responsabilità delle persone giuridiche che, in forza dell'art. 10, gli Stati parte hanno l'obbligo di introdurre per la partecipazione a reati gravi che coinvolgono un gruppo criminale organizzato.

In particolare, si avverte la necessità di specificare a quali condizioni gli intermediari di Internet possano essere ritenuti responsabili per reati gravi commessi attraverso le loro reti e servizi.

La questione richiede necessariamente di essere affrontata a livello internazionale. Essendo Internet una rete globale di servizi interconnessi, le misure di responsabilità degli intermediari in uno Stato producono inevitabilmente effetti anche in altri Stati. Eppure, in questa materia si registra la mancanza sia di strutture di cooperazione internazionale, sia di dati affidabili sulla base dei quali valutare l'efficacia e la proporzionalità delle misure da adottare[30].

Una sede adeguata per le proposte riguardanti la responsabilità degli intermediari e la cooperazione con gli stessi per combattere la criminalità transnazionale è l'attività di gestione e implementazione della Convenzione di Palermo, affidata

---

[27] UNODC, *Digesto di casi di criminalità organizzata, raccolta commentata di casi e lezioni apprese*, Nazioni Unite, 2012, p. 18.

[28] C. PONTI, *op. cit.*, pp. 72 ss.

[29] Si consenta un rinvio a A. MATTARELLA, *La responsabilità delle persone giuridiche*, in *La Convenzione di Palermo*, op. cit., pp. 375 ss.

[30] In questo senso v. il Rapporto dal titolo "*The age of digital interdependence*" predisposto nel 2019 dall'*High-Level Panel on Digital Cooperation* del Segretario generale delle Nazioni Unite.

all'UNODC. In tale ambito, si stanno sviluppando una serie di iniziative innovative in applicazione dell'art. 28 della Convenzione, che incoraggia gli Stati a:

a) analizzare, con la consulenza della comunità accademica e scientifica, le tendenze della criminalità organizzata e le tecnologie da essa utilizzate;
b) sviluppare e condividere attraverso le organizzazioni internazionali le conoscenze analitiche così acquisite, in vista della elaborazione ed applicazione di definizioni, standard e metodologie comuni;
c) monitorare e valutare le proprie politiche criminali e le misure attuative.

Si tratta, dunque, di una norma giuridica programmatica che crea una stretta continuità tra analisi dei fenomeni criminali, con specifico riferimento all'uso della tecnologia per attività illecite, elaborazione delle politiche di contrasto e monitoraggio della loro efficacia. Da tale norma può scaturire un importante processo di innovazione, per razionalizzare tutte le misure di contrasto alle forme gravi di cybercriminalità nel rispetto degli standard internazionali relativi alle libertà di pensiero ed espressione.

Nella più recente attività delle Nazioni Unite sono state approfondite particolarmente le tematiche della responsabilità degli intermediari di Internet, delle condizioni per l'esenzione da responsabilità, e delle altre tipologie di cooperazione sostenute dagli intermediari di Internet, tenendo conto dell'esperienza acquisita a livello nazionale e internazionale, nonché delle varie forme di autoregolamentazione, di coregolamentazione e di privatizzazione.

La questione della responsabilità giuridica degli intermediari di Internet ha formato a lungo oggetto di dibattito. Alcuni casi giudiziari verificatisi tra la fine del secolo scorso e l'inizio dell'attuale assumono in proposito un indubbio valore emblematico[31]. In una fase storica in cui il potenziale economico e sociale di Internet emergeva in modo sempre più ampio, una situazione di incertezza giuridica era insostenibile sia per le autorità pubbliche, che avevano bisogno di conoscere le misure esigibili dagli intermediari, sia per gli utilizzatori dei servizi *online*, che intendevano accedere a tali servizi legalmente per esercitare i loro diritti civili, economici e politici,

[31] Già nel 1993, CompuServe, allora il secondo più grande servizio online al mondo, venne citato in giudizio per violazione del *copyright* sulle sue reti, mentre nel 1998 l'amministratore delegato di CompuServe Germania venne condannato a due anni di reclusione, essendo stato ritenuto responsabile per il materiale relativo ad abusi su minori a cui si accedeva sui suoi server. Tale statuizione venne poi ribaltata in appello per la mancanza di adeguate tecnologie preventive. Nel 2000, il caso Yahoo! Francia sollevò altre complesse questioni sul rapporto tra responsabilità e tecnologia. Ci si chiedeva, in particolare, se Yahoo! Francia fosse responsabile per il fatto che la casa madre, usando server negli Stati Uniti, avesse messo all'asta oggetti (precisamente, si trattava di cimeli) vietati dalla legge francese, così da consentire agli utenti francesi di accedere a un servizio che offriva in vendita articoli illegali secondo la normativa del loro paese. In questo caso, l'autorità giudiziaria osservò che Yahoo! aveva fornito pubblicità in francese ai visitatori francesi del sito e quindi la sua condotta non era del tutto passiva; si pose quindi a carico di Yahoo! Francia un obbligo di bloccare gli indirizzi IP francesi così da limitare l'accesso degli utenti francesi. Alla fine, Yahoo! decise che il mantenimento delle vendite dei cimeli richiedeva uno sforzo eccessivo e lo rimosse del tutto. Quest'ultimo caso è considerato particolarmente importante perché in esso furono presi in esame il livello di "conoscenza" dell'attività illegale, la volontà di imporre soluzioni tecniche limitate e l'impatto extraterritoriali di decisioni giudiziarie emesse in altri Stati.

sia per i fornitori di servizi *online*, che necessitavano di una chiara comprensione dei rischi legali connessi alla loro attività.

A questi problemi hanno cercato di dare una risposta il *Communications Decency Act* (CDA) del 1996 e il *Digital Millenium Copyright Act* (DMCA) del 1998 negli Stati Uniti e la Direttiva sul commercio elettronico del 2000 nell'Unione Europea.

La Sezione 230 del *Communications Decency Act* ha garantito, in linea di principio, l'immunità dalla responsabilità per gli intermediari di Internet, stabilendo che nessun fornitore e nessun utilizzatore di servizi Internet può essere considerato responsabile, come editore o autore, di una qualsiasi informazione fornita da terzi. Tale previsione non impone alcun dovere di rimozione in capo agli intermediari della rete, neppure nel caso di omessa risposta alle comunicazioni loro indirizzate; resta parimenti esclusa la loro responsabilità per la limitazione dell'accesso ai contenuti *online*, qualora tale restrizione sia stata attuata in buona fede in correlazione con gli obiettivi perseguiti dalla normativa, consistenti nella introduzione di limiti ai contenuti illegali. A sua volta, il *Digital Millennium Copyright Act* ha escluso la responsabilità per violazioni del *copyright* dei fornitori di servizi *online* che rispondano prontamente alle comunicazioni dei proprietari dei diritti o dei loro agenti volte a bloccare l'accesso a contenuti presumibilmente lesivi e si conformino agli ordini giudiziari finalizzati ad ottenere l'accesso alle informazioni relative agli utenti.

Questi due testi normativi statunitensi hanno fortemente influenzato la "Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno", che tuttavia presenta alcune differenze di disciplina. Precisamente, le eccezioni alla responsabilità riguardano specificamente quegli intermediari i cui servizi comportano l'accesso a Internet ("*mere conduit*"), implicano la "memorizzazione temporanea" ("*caching*") o consistono nell' "ospitare" contenuti per terzi ("*hosting*"). Con riferimento a queste tre categorie, la direttiva esclude che gli Stati membri impongano ai prestatori di servizi internet un obbligo generale di sorveglianza sulle informazioni che trasmettono o memorizzano ovvero un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite.

A differenza del *Communications Decency Act*, nella direttiva non viene prevista una esenzione di responsabilità per le restrizioni "in buona fede" all'accesso ai contenuti. Diversamente dal *Digital Millennium Copyright Act*, che è limitato alle violazioni del *copyright*, la Direttiva riguarda la responsabilità per tutti i tipi di contenuti illegali.

In forza dell'art. 14 della Direttiva, nel caso di "*hosting*" la esclusione di responsabilità del prestatore di servizi consistenti nella memorizzazione di informazioni fornite dai destinatari del servizio è subordinata a una duplice condizione:

a) che il prestatore non sia effettivamente a conoscenza della illiceità dell'informazione; e

b) che il prestatore agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso, non appena venuto a conoscenza della loro natura illecita.

La Direttiva ha favorito in modo significativo la cooperazione degli intermediari, segnatamente mediante la istituzione e il finanziamento di una rete internazionale di *hotlines* per la segnalazione di contenuti criminali nel settore dell'abuso su minori.

Alla suesposta produzione normativa non ha però ancora fatto seguito la costruzione di un quadro internazionale di regolamentazione, che prenda in considerazione l'esatta natura di ciascun tipo di intermediario, il tipo di poteri impeditivi di cui esso dispone, e i criteri di attribuzione della responsabilità.

Su quest'ultimo profilo, si riscontrano previsioni molto diverse nelle legislazioni nazionali, in collegamento con le differenti tradizioni giuridiche in materia di colpevolezza.

In generale, nelle legislazioni nazionali sono emersi due modelli principali di responsabilità delle persone giuridiche: il modello "derivativo", che fa discendere la responsabilità dell'ente da quella delle persone attraverso cui esso agisce, e il modello "organizzativo", che si concentra sulla "colpa" della stessa organizzazione, analizzando la sua struttura, le sue politiche di impresa e le sue eventuali carenze nel controllo sui dipendenti e su altri agenti.

Generalmente, in tutte le situazioni in cui non vi è il coinvolgimento diretto di un intermediario nella commissione di reato, la responsabilità delle persone giuridiche è basata sulla mancata adozione dei comportamenti doverosi che appaiono idonei a prevenire o a far cessare il compimento di attività illecite. Appare, però, difficile la prova della colpa degli intermediari nel caso in cui manchino precise segnalazioni di specifiche attività illecite.

Resta problematica la individuazione delle ipotesi in cui un intermediario di Internet abbia motivi ragionevoli per ritenere che i suoi servizi vengano utilizzati per reati gravi che coinvolgono un gruppo criminale organizzato, nonché della definizione delle misure esigibili per impedire che il servizio venga utilizzato per tale scopo. Ad esempio, nel caso in cui il singolo contenuto illegale rappresenta semplicemente un elemento di una più ampia attività criminale, la unilaterale rimozione di esso da parte dell'intermediario di Internet, avvisato da un soggetto privato, potrebbe avere persino un effetto pregiudizievole per le indagini condotte dagli organi investigativi. E' indubbia quindi l'importanza essenziale di un maggiore coordinamento tra gli intermediari di internet e le autorità giudiziarie e di polizia al fine di rafforzare la lotta contro una criminalità organizzata ormai "addestrata" all'uso dei sistemi telematici.

Per tutte le suesposte ragioni, evidenziate nelle più recenti iniziative dell'UNODC, sta progressivamente affermandosi l'indirizzo favorevole a una nuova regolamentazione della responsabilità degli intermediari di Internet, costruita in termini idonei ad accrescere l'efficacia del contrasto alla criminalità organizzata, la tutela dei diritti fondamentali e la certezza del diritto, con un impatto positivo anche sul piano della libertà di iniziativa economica degli operatori. Alla luce degli interessi in gioco, la responsabilità delle persone giuridiche deve essere ancorata ad un quadro normativo certo e tendenzialmente uniforme per tutti gli intermediari che operano nello stesso mercato: un traguardo che non è stato ancora raggiunto.

È propria in questa direzione che il nuovo progetto di Convenzione dell'Onu sul cybercrime potrebbe incidere sensibilmente, normando con maggiore precisione i margini di responsabilità degli operatori e le relative garanzie giurisdizionali.

4. L'importanza di una Convenzione Onu in materia di *cybercrime* e il lungo percorso verso la firma.

Alla luce di quanto si è visto, è essenziale un nuovo strumento giuridico internazionale che rilanci la battaglia contro il crimine informatico e faccia sintesi delle necessarie innovazioni nell'ottica di una possibile armonizzazione degli ordinamenti a livello globale. Come si è anticipato, nella fase attuale, gli Stati partecipanti hanno espresso le loro posizioni in merito presentando delle proposte al Comitato. Giova quindi esaminare in modo più approfondito gli orientamenti delle principali potenze mondiali come gli Stati Uniti, il Regno Unito, la Cina, la Russia e l'Unione Europea.

Negli ultimi anni, gli Stati si sono avvicinati al tema della "sovranità digitale" e della regolamentazione dei dati digitali e delle relative infrastrutture nel proprio territorio. Storicamente, Russia e Cina sono stati i principali esempi. Le autorità russe hanno recentemente arrestato gli amministratori delegati di alcune società di sicurezza informatica con l'accusa di tradimento[32], mentre le autorità di regolazione cinesi hanno limitato il potere delle aziende tecnologiche imponendo multe e ristrutturazioni alle grandi aziende.[33]

Di recente, anche i paesi dell'UE hanno compiuto alcuni passi significativi sul tema della "sovranità digitale". Sebbene in precedenza gli Stati occidentali prediligessero "un modello di governance multi-stakeholder, inclusivo dei soggetti privati, come le società di telecomunicazione"[34], sempre più questi paesi mirano ad estendere i controlli nei confronti di tali società, in particolare quando hanno sedi all'estero. Anche negli Stati occidentali, le aziende tecnologiche hanno soddisfatto le richieste di trasparenza dei paesi in cui operano. I governi vantano ora un maggiore controllo delle tecnologie informatiche o hanno capacità che consentono loro di implementare misure come la chiusura di Internet, indipendentemente dalla conformità da parte delle aziende tecnologiche.

Un'indagine congiunta del progetto Jigsaw di Google, Access Now e Censored Planet ha scoperto che delle quasi 850 chiusure intenzionali di Internet documentate negli ultimi 10 anni, 768 sono avvenute in 63 paesi a partire dal 2016[35]. Solo nel 2020,

---

[32] T. BALMFORTH, A. ZVEREV, *Russia arrests top cybersecurity executive in treason case*, Reuters, 29 September 2021, in www.reuters.com.

[33] K. WU, J. ZHU, *Billionaire Alibaba founder Jack Ma reappears in Hong Kong*, Reuters, 13 October 2021, in www.reuters.com.

[34] S. WALKER, *Cyber insecurities? A guide to the UN cybercrime debate*, GI-TOC, 2019, pp 6–7, in www.globalinitiative.net.

[35] T. RYAN-MOSLEY, *Why you should be more concerned about internet shutdowns*, MIT Technology Review, 9 September 2021, in www.technologyreview.com; UNITED NATIONS HUMAN RIGHTS COUNCIL, *Ending Internet shutdowns: a path forward*, United Nations, 15 June 2021, in www.undocs.org.

quando la maggior parte del mondo era in stato di emergenza per il COVID-19, affidandosi ad Internet per le comunicazioni e le esigenze di base, sono stati segnalati 155 blocchi di Internet in 29 paesi[36].

Sebbene la comunità internazionale sia generalmente favorevole all'estensione dei poteri di intervento dei governi, i paesi differiscono intorno ai modi ed alle ragioni di tali politiche e ciò avrà un impatto sui negoziati.

Già dal 12° Congresso delle Nazioni Unite sulla Prevenzione della criminalità e la Giustizia penale tenutosi in Brasile nel 2010, alcuni paesi tra cui la Russia avevano proposto un nuovo trattato sulla criminalità informatica all'interno del sistema delle Nazioni Unite. Ciò ha portato alla creazione del gruppo intergovernativo di esperti (IEG) per condurre uno studio completo sulla criminalità informatica, che ha operato fino al 2021 nell'ambito della Commissione delle Nazioni Unite per la Prevenzione della Criminalità e la Giustizia Penale (CCPCJ).

Nel 2017, la Russia ha nuovamente presentato al segretario generale della Nazioni Unite una bozza di convenzione sulla criminalità informatica.

Nel 2019, come si è detto, la Risoluzione 74/247 è stata approvata dall'Assemblea Generale delle Nazioni Unite, con 79 voti a favore, 60 voti contrari e 33 astenuti.

Sebbene il processo di elaborazione della nuova Convenzione ONU inizi sul piano tecnico solo nel 2022, gli incontri svoltisi nel corso del 2021 hanno già messo in luce le tensioni che caratterizzano i negoziati.

Nell'ambito della sessione organizzativa del maggio 2021, i negoziati si sono rivelati molto controversi, non solo tra i Paesi che avevano votato originariamente per la risoluzione 74/247, ma anche tra gli Stati che volevano un processo decisionale più inclusivo e trasparente, con il coinvolgimento della società civile. In particolare, il Regno Unito e la Svizzera hanno ritenuto che le proposte presentate non fossero sufficientemente inclusive per la società civile. Gli interventi effettuati dal Brasile, dai paesi del CARICOM e dal Regno Unito hanno portato alla presentazione di tre emendamenti alla proposta di delibera. Gli emendamenti presentati da Brasile e Regno Unito sono stati approvati mediante votazione, mentre quelli di Haiti attraverso la procedura per *consensus*. Con le modifiche citate, la risoluzione russa è stata adottata senza votazione, sulla base di un'accettazione generale[37].

Come anticipato, si è stabilito che la prima sessione negoziale del comitato *ad hoc* si svolga dal 28 febbraio all'11 marzo 2022 a New York, nel formato "ibrido" (cioè con duplice modalità di partecipazione, sia di presenza sia online) determinato dalla pandemia. Si sta formando un accordo sulla individuazione delle Organizzazioni non governative e istituzioni accademiche che potranno partecipare ai lavori in aggiunta alle ONG già dotate di status consultivo presso l'ECOSOC. Ma si riscontra tuttora una generale mancanza di un accordo sostanziale su quale dovrebbe essere l'ambito di applicazione della convenzione.

---

[36] AccessNow, #KeepItOn, in www.accessnow.org.

[37] Per ripercorrere le tappe dei negoziati, v. S. WALKER – I. TENNANT, *Control, Alt, or Delete? The Un cyber crime debate enters a new phase,* Global initiative against transnational organized crime, December 2021.

4.1. Le relazioni presentate dagli Stati e la posizione dei principali "players" globali: gli U.S.A.

Entrando nel merito delle posizioni espresse, il Governo degli Stati Uniti d'America ha risposto all'invito rivolto agli Stati membri a presentare le proprie opinioni sulla portata, gli obiettivi e la struttura della nuova convenzione, sottolineando l'urgenza di elaborare uno strumento globale incentrato sul miglioramento delle indagini e del perseguimento della criminalità informatica, coerente e basato sui diritti e gli obblighi esistenti. I rappresentanti americani hanno sottolineato l'importanza di un negoziato aperto, inclusivo, trasparente e basato sul consenso, in modo da pervenire ad un'adesione diffusa. In particolare, il Governo degli USA ha rimarcato come la pandemia abbia accelerato l'utilizzazione, da parte delle organizzazioni criminali, degli strumenti informatici. In questo senso, la percentuale di attacchi hacker e di reati informatici è aumentata esponenzialmente. Il crimine organizzato ha saputo abilmente sfruttare il cambiamento globale e la dipendenza dalle tecnologie digitali. Per tali ragioni, la criminalità informatica è una minaccia diretta alla sicurezza e al benessere delle società e delle persone in tutto il mondo. Data l'immediatezza della minaccia, è ancora più essenziale negoziare uno strumento globale contro il crimine informatico. La nuova Convenzione dovrebbe mirare a rafforzare la cooperazione internazionale e fornire alle autorità nazionali strumenti pratici per contrastare la criminalità informatica, come hanno fatto altri strumenti delle Nazioni Unite per varie forme di criminalità transnazionale, come la corruzione, il traffico di stupefacenti, la tratta di esseri umani e il traffico di migranti. Secondo i rappresentanti americani, in particolare, la futura Convenzione dovrebbe anche valorizzare la ricerca delle prove rilevanti attraverso strumenti elettronici non solo per il cybercrime, ma per qualsiasi tipo di reato.

D'altra parte, si segnala che, come avviene per ogni strumento di contrasto al crimine organizzato, è necessario includere limiti e garanzie appropriate, nei sistemi nazionali, per la privacy e gli altri diritti umani. Soprattutto, gli Stati Uniti evidenziano l'importanza del tema dell'assistenza tecnica e della cooperazione tra gli Stati in funzione di ausilio dei paesi dotati di minori risorse tecnologiche.

Un'importante presa di posizione è quella secondo la quale gli Stati membri non dovrebbero approfondire gli argomenti relativi alla *governance* o alla sicurezza informatica in uno strumento penale dedicato alla lotta alla criminalità informatica. In tale prospettiva, sebbene spesso i due profili siano visti come due facce della stessa medaglia, la repressione della criminalità informatica sarebbe essenzialmente una responsabilità dello Stato, mentre la sicurezza informatica dovrebbe essere affidata alla responsabilità condivisa di una serie di attori pubblici e privati.

Pertanto gli Stati Uniti sottolineano che il mandato del Comitato *ad hoc* è incentrato sullo sviluppo di uno strumento penale che faciliti una risposta internazionale alla criminalità informatica, attraverso la definizione e la sanzione delle condotte criminali nel cyberspazio. Esso non avrebbe, invece, il potere di dettare norme globali di condotta per gli operatori in ambito informatico. L'inclusione dei concetti di *governance* informatica e sicurezza informatica in un trattato sulla criminalità informatica

ostacolerebbe l'obiettivo di uno strumento efficace, ampiamente sostenuto da parte degli Stati membri.

Ancora, gli USA sottolineano che, come riaffermato nella risoluzione 75/282 dell'Assemblea generale, è fondamentale che i negoziati non pregiudichino i meccanismi multilaterali e regionali già esistenti che già consentono di combattere efficacemente la criminalità informatica.

In proposito, si fa riferimento a trattati delle Nazioni Unite come la Convenzione di Palermo contro il crimine organizzato transnazionale, che colpisce attività fondamentali della criminalità organizzata e detta disposizioni di cooperazione internazionale che possono essere applicate a qualsiasi tipo di reato grave commesso a scopo di lucro da tre o più persone. Come già visto in precedenza, i rappresentanti americani evidenziano che gli Stati hanno già utilizzato con successo la Convenzione di Palermo anche contro i crimini informatici, con particolare riferimento all'uso di *ransomware* ed allo sfruttamento sessuale dei minori. Questi decenni di esperienza nelle indagini sulla criminalità informatica dimostrano l'efficacia di una strategia condivisa degli Stati membri, per evitare la creazione di zone franche per i criminali informatici.

Inoltre, il Governo statunitense puntualizza che il nuovo strumento dovrebbe rimarcare la distinzione tra i reati cyber-dipendenti, in cui un computer o i dati sono l'obiettivo dell'attività criminale, e i reati cyber-correlati, in cui le tecnologie informatiche sono lo strumento che agevola il delitto.

I crimini cyber-dipendenti, la prima categoria a cui dovrebbe rivolgersi principalmente la nuova Convenzione, possono avvenire completamente nel mondo digitale e sono quelli che non esistevano prima dell'avvento dei sistemi informatici, non potendo essere commessi senza l'uso improprio di computer o sistemi di rete. Per questi reati legati alla criminalità informatica, come gli attacchi hacker o il danneggiamento di dati o sistemi informatici, sono necessarie normative specifiche in quanto nella maggior parte delle giurisdizioni le leggi penali applicabili ai reati commessi al di fuori di una rete informatica potrebbero non essere applicabili alle condotte commesse nella realtà virtuale.

Per converso, i rappresentanti americani segnalano il rischio di estendere la disciplina dei cybercrime ai reati tradizionali per il semplice fatto che un computer è stato coinvolto nella loro esecuzione. Occorrerà quindi distinguere, nel novero delle fattispecie tradizionali, quelle non compatibili con le nuove tecnologie dalle forme di criminalità, come la frode, lo sfruttamento minorile, e la diffamazione, che potrebbero essere considerati nell'ambito della negoziazione della Convenzione, in quanto l'uso di un computer aumenta la portata offensiva del reato, la velocità della lesione, l'entità del pregiudizio alle vittime o l'anonimato dell'autore.

Inoltre, secondo gli USA, una Convenzione dotata di una vocazione universale dovrebbe punire i reati informatici in modo tecnologicamente neutro, incriminando l'attività che pregiudica la riservatezza, l'integrità e la disponibilità dei dati informatici invece di selezionare la particolare forma o metodo utilizzato, come il *phishing* o il *ransomware*. Al contempo le disposizioni della Convenzione devono essere adattabili non solo alle tecnologie del presente, ma anche ai nuovi strumenti emergenti in futuro. A dimostrazione della rapidità con cui la tecnologia si sviluppa, i rappresentanti

americani citano anche il *Draft Comprehensive Study on Cybercrime* del 2013, che, pur proponendosi di essere completo, mancava di dettagli su tecnologie o tecniche che non erano ampiamente utilizzate, o erano semplicemente emergenti, al momento dello studio, inclusi i *ransomware*, le criptovalute e il rapido sviluppo e predominio della tecnologia mobile e dei social. Pertanto, affinchè le disposizioni in esame resistano alla prova del tempo, occorre emanare normative con formulazioni tecnologicamente neutrali e criminalizzare l'attività ritenuta illegale invece dei mezzi utilizzati[38]. Ciò è particolarmente importante anche per soddisfare le esigenze degli operatori del diritto e delle forze dell'ordine in futuro. Si tratta di un elemento valorizzato in precedenza riguardo alla Convenzione di Palermo. All'uopo, le formulazioni degli accordi internazionali sono caratterizzate da una certa ampiezza e flessibilità non solo per l'inevitabile compromesso tra le diverse posizioni degli Stati, ma anche per scongiurare il rischio di naturale obsolescenza normativa.

In virtù dei principi espressi, gli Stati Uniti concludono sostenendo la necessità di includere nella Convenzione sul Cybercrime alcune fattispecie, come l'accesso illegale a un computer o a un sistema informatico senza autorizzazione, l'intercettazione illecita del contenuto delle comunicazioni o dei dati di traffico relativi alle comunicazioni, l'interferenza sui dati o sul sistema, ovvero *malware*, attacchi *Denial of Service*, *ransomware*, cancellazione o modifica dei dati, il traffico o utilizzo di dati di carte di credito, password e informazioni personali, reati relativi a materiale pedopornografico, frodi informatiche, quali *phishing*[39], compromissione della posta elettronica aziendale, violazioni del diritto d'autore e contraffazione di marchi. Infine, in tutte le ipotesi descritte, dovrebbero essere previste delle forme di confisca dei proventi illecitamente accumulati.

*4.2. (*segue*) Il Regno Unito.*

Di particolare interesse è anche la relazione presentata dal Regno Unito, che evidenzia come la nuova convenzione dovrebbe concentrarsi soprattutto sul rafforzamento della cooperazione per affrontare la crescente minaccia che le attività virtuali rappresentano per i cittadini, per le imprese e i governi. Sotto tale profilo, specie alla luce della crescita del commercio elettronico, il cybercrime rischia di pregiudicare la libertà di concorrenza e lo sviluppo economico.

Il governo britannico ha posto in evidenza i successi raggiunti in materia penale nell'ambito delle Nazioni Unite, attraverso la Convenzione di Merida del 2005 contro la corruzione (UNCAC) e la già citata Convenzione di Palermo del 2000 contro la

---

[38] UNODC/CCPCJ/EG.4/2021/2, Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime tenutosi a Vienna dal 6 all'8 aprile 2021, disponibile su www.unodc.org.

[39] Per le problematiche sollevate dal fenomeno del *phishing*, v. R.FLOR, *Phishing, Identity theft e identity abuse. Le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. e proc. pen*., n. 2-3/ 2007, p. 899.

criminalità organizzata transnazionale (UNTOC). In quest'ottica, si afferma che il nuovo strumento dovrà coordinarsi con le disposizioni previgenti, in modo da costruire un sistema normativo coerente. Scopo del trattato dovrebbe essere anche il potenziamento delle indagini e delle sanzioni per i reati informatici. Nella specie, viene considerato prioritario lo sviluppo delle capacità professionali degli operatori per consentire a tutti gli Stati membri delle Nazioni Unite di affrontare questi reati, insieme all'istituzione di un gruppo di esperti attraverso il quale possano essere identificati gli attacchi informatici. Ai fini di un'efficace cooperazione, è necessario che le fattispecie di reato introdotte siano riconosciute da tutti gli ordinamenti giuridici. Allo stesso tempo, il governo britannico auspica che la nuova disciplina non pregiudichi l'esercizio dei diritti fondamentali, come in particolare la libertà di espressione. Come per ogni Convenzione, occorrono solide garanzie che includano il rispetto della privacy e di altri diritti umani, come stabilito dal diritto internazionale umanitario e riconosciuto nelle pertinenti risoluzioni adottate dall'Assemblea generale e dal Consiglio per i diritti umani delle Nazioni Unite. Sono quindi necessari meccanismi di rifiuto dell'estradizione per violazione del *ne bis in idem*, quando il presunto reato riguarda l'esercizio della libertà di espressione e quando la richiesta di consegna ha lo scopo di punire o perseguitare l'individuo per motivi di razza, religione, sesso o motivi politici. A tal fine, si richiede un approccio inclusivo e "*multi-stakeholder*", aperto all'intervento di cittadini, organizzazioni non governative, società civile, istituzioni accademiche e aziende private.

Su due ulteriori aspetti, sembra configurarsi una posizione comune a quella espressa dagli Stati Uniti. In primo luogo, anche la relazione del Regno Unito ritiene che debba esulare dal futuro accordo la materia della sicurezza informatica e della *governance* di Internet. In secondo luogo, si sostiene l'importanza di una formulazione il più possibile aperta e tecnologicamente neutrale per evitare la necessità di continui aggiornamenti della disciplina e assicurarsi che la Convenzione rimanga al passo con i tempi.

Degno di nota è il riferimento dei rappresentanti britannici all'istituzione in ogni paese di agenzie investigative indipendenti dotate di competenze nel contrasto alla criminalità informatica, con la capacità di valutare il livello della minaccia e i provvedimenti adeguati. In una materia caratterizzata da elevato tecnicismo e dall'esigenza di continui aggiornamenti, il modello delle autorità indipendenti, sperimentato su larga scala negli ordinamenti angloamericani e, più di recente, anche nei principali paesi europei, può rappresentare un utile strumento per implementare il sistema normativo, il quale non potrà prescindere da un'attività di regolazione e di fissazione di buone pratiche rivolte agli attori del web.

Da ultimo, il Regno Unito delinea la possibile struttura del trattato, che dovrebbe contenere, in primo luogo, le disposizioni generali sullo scopo della normativa e le definizioni da utilizzare, che devono essere tecnologicamente neutrali, tenendo conto dei quadri giuridici nazionali. In secondo luogo, tra le fattispecie da perseguire, occorrerebbe recepire la distinzione tra reati cyber-dipendenti (come l'accesso illegale) e cyber-correlati, attraverso definizioni accettabili per tutte le parti contraenti. Ancora, dovrebbe essere dedicata specifica attenzione alle misure preventive, come avviene per la Convenzione di Merida contro la corruzione e per la Convenzione di Palermo contro

il crimine organizzato, incoraggiando l'assistenza tecnica e il rafforzamento delle capacità dei singoli Stati dotati di minori risorse tecnologiche, attraverso un coordinamento con strutture esistenti come il Forum globale sulla competenza informatica (GFCE). In tal senso, si fa riferimento, tra gli altri, al ruolo significativo dell'Ufficio delle Nazioni Unite contro la droga e il crimine (UNODC), ed al gran numero di raccomandazioni adottate dal Gruppo intergovernativo di Esperti (IEG) nell'aprile 2021, incentrate sullo sviluppo della formazione specialistica per gli operatori che indagano sulla criminalità informatica, in particolare sulla gestione delle prove elettroniche.

*4.3. (*segue*) L'Unione Europea.*

Proseguendo nell'esame delle proposte presentate, è importante esaminare la posizione dell'Unione europea.

A tal riguardo, occorre premettere che, con l'entrata in vigore del Trattato di Lisbona, la "criminalità informatica" è stata inserita nell'art. 83 TFUE fra i fenomeni criminosi di natura grave e transnazionale sui quali l'Unione Europea ha competenza penale. Come ha già da prima affermato la Corte di giustizia, a partire dal 2005, l'Unione non ha una competenza diretta in materia penale, ma ciò non impedisce di elaborare norme sostanziali relative alla definizione dei reati e delle pene quando ciò sia necessario per contrastare sfere di criminalità particolarmente gravi di dimensione transnazionale. Un ruolo fondamentale, in questo processo di "europeizzazione" del contrasto al crimine organizzato, può essere rivestito dalla Procura Europea, che è stata istituita nel 2017. Sebbene le competenze del nuovo organo siano state originariamente limitate alla repressione delle frodi lesive degli interessi finanziari dell'Unione, ai sensi degli artt. 83 e 86 TFUE è possibile estendere la sua sfera di intervento ai "*serious crimes having a cross border dimension*".

Si tratta di una prospettiva auspicata da buona parte della dottrina tanto in relazione alla crescente diffusione delle ecomafie, quanto in riferimento alle altre tipologie di crimine organizzato, nelle quali rientra oggi a pieno titolo anche il cybercrime. A ben vedere, questi ultimi sono già oggetto dell'attenzione dei Procuratori europei, considerando che una notevole parte delle frodi viene commessa avvalendosi di mezzi informatici.

Ciò premesso, i rappresentanti dell'Unione affermano che la loro proposta non pregiudica eventuali posizioni future che l'UE e i suoi Stati membri potrebbero assumere nel corso dei negoziati sulla portata, gli obiettivi e la struttura della Convenzione delle Nazioni Unite sul cybercrime.

Secondo l'Unione Europea, gli obiettivi principali dovrebbero essere la previsione di strumenti pratici per il contrasto dei reati e l'implementazione della cooperazione tra le autorità giudiziarie nella lotta globale contro la criminalità informatica. Come si evince dalle risoluzioni 74/247 e 75/2823 dell'Assemblea Generale dell'ONU (UNGA), la Convenzione dovrebbe integrare il quadro giuridico esistente di strumenti internazionali e regionali nel campo della criminalità organizzata e della

cybercriminalità, al fine di non pregiudicare l'applicazione degli strumenti vigenti o l'adesione di altri paesi e di evitare duplicazioni.

La futura Convenzione delle Nazioni Unite, come concordato dalla risoluzione 75/282 dell'UNGA, dovrebbe tenere in piena considerazione il lavoro e i risultati del gruppo intergovernativo di esperti (IEG) per condurre uno studio completo sulla criminalità informatica.

In relazione al campo di applicazione del nuovo strumento, l'UE e i suoi Stati membri ritengono che esso dovrebbe concentrarsi principalmente sulle fattispecie penali sostanziali da perseguire e sui relativi meccanismi di procedura e di cooperazione. Tali disposizioni dovrebbero in generale riguardare solo i reati ad alta tecnologia e i reati cyber-dipendenti, come l'accesso illegale, l'intercettazione o l'interferenza con dati e sistemi informatici. Le disposizioni sostanziali di diritto penale devono essere definite in modo chiaro e ristretto ed essere pienamente compatibili con gli standard internazionali sui diritti umani e con un cyberspazio globale, aperto, libero e sicuro.

A tal riguardo, disposizioni che criminalizzano condotte non chiaramente definite rischierebbero di interferire in modo indebito e sproporzionato con i diritti umani e le libertà fondamentali, compresa la libertà di espressione, determinando imprevedibilità anche per gli operatori economici.

Le disposizioni di diritto penale sostanziale dovrebbero, per quanto possibile, essere redatte in modo tecnologicamente neutro al fine di comprendere gli sviluppi tecnici del futuro[40]. Dovrebbero inoltre rispettare gli standard internazionali sui diritti umani e proteggere altresì le vittime.

In tale ottica, l'azione di contrasto deve essere ancorata ad adeguate garanzie procedurali nel rispetto dei principi di necessità e proporzionalità, per tutelare in particolare il diritto alla riservatezza e alla protezione dei dati personali, la libertà di espressione e di informazione e il diritto a un processo equo, ad un livello almeno pari alle garanzie di altri strumenti internazionali. Allo stesso tempo dovrebbe essere incoraggiato lo scambio di opinioni e informazioni sulle nuove sfide poste da ulteriori sviluppi tecnologici.

In generale, la futura Convenzione delle Nazioni Unite dovrebbe astenersi dal fissare standard minimi sanzionatori o pene per reati specifici al di là dei modelli esistenti.

Per quanto riguarda le norme sulla giurisdizione, la futura Convenzione delle Nazioni Unite dovrebbe essere modellata sull'approccio stabilito negli strumenti giuridici esistenti, come l'articolo 15 della già citata Convenzione di Merida.

Tra le misure di cooperazione tra le parti è compresa la cooperazione investigativa e giudiziaria, con riferimento alla ricerca, conservazione, autenticazione e utilizzazione di prove elettroniche[41]. Ad avviso dei rappresentanti europei, inoltre, nella struttura della Convenzione dovrebbe essere inserita una disciplina specifica per l'assistenza tecnica, la formazione e lo sviluppo delle competenze.

---

[40] Cfr. la raccomandazione 1 adottata su Legislazione e quadri normativi dall'IEG.

[41] Cfr. la raccomandazione 16 adottata sull'evidenza elettronica e la giustizia penale dell'IEG.

Si fa riferimento, in particolare, alle attività fondamentali svolte dall'UNODC ai fini dell'implementazione della Convenzione di Palermo, nei settori delle tecniche investigative, della condivisione delle migliori pratiche e dell'assistenza. L'art. 29 della Convenzione di Palermo obbliga gli Stati ad avviare programmi di formazione dei funzionari e di prestare assistenza ad altri paesi, soprattutto nella lotta alla criminalità organizzata transnazionale che utilizza computer, reti di telecomunicazioni o altre forme di tecnologia moderna. Si tratta di un aspetto centrale nel contrasto al cybercrime, in quanto lo scambio di informazioni e di personale può incentivare lo sviluppo di una cultura condivisa tra gli operatori giuridici.

Infine, l'Unione europea sostiene che debbano essere escluse dal campo di applicazione della futura Convenzione delle Nazioni Unite le questioni relative alla sicurezza nazionale ed alla *governance* di Internet, che sono oggetto di politiche e di incontri settoriali. Inoltre, trattandosi di uno strumento intergovernativo, non dovrebbero imporsi direttamente degli obblighi alle organizzazioni private, compresi gli organismi non governativi e i fornitori di servizi Internet.

Si può qui riscontrare una posizione comune a quella degli Stati Uniti e del Regno Unito, caratterizzata dalla preoccupazione di non paralizzare con regole eccessivamente rigide il settore del commercio elettronico.

Si profila, dunque, un doppio binario, uno riguardante gli obblighi dei pubblici poteri di prevenire e punire il crimine cibernetico, l'altro attinente alla sfera della *governance* del web, tendenzialmente regolato da minori vincoli e con una maggiore libertà di azione dei soggetti privati.

Si tratta forse della questione più importante che le future legislazioni contro il cybercrime saranno chiamate ad affrontare, quella del bilanciamento tra autorità e libertà, tra regolazione e iniziativa privata, in quanto la repressione dei reati non deve vanificare le conquiste raggiunte grazie al mondo di Internet.

*4.4. (*segue*) La Russia.*

Più estese e articolate sono le relazioni presentate dalla Cina e dalla Russia.

La relazione della Russia è, sostanzialmente, un vero e proprio schema di Convenzione.

I rappresentanti russi esprimono, in tal senso, la preoccupazione che l'abuso delle tecnologie abbia ampliato le possibilità delle attività criminali, facendo riferimento soprattutto a fenomeni come gli attacchi informatici ad infrastrutture critiche, lo spionaggio informatico, la pedofilia *online*, lo sfruttamento dei minori, il terrorismo, la frode, il traffico di dati personali e il riciclaggio di denaro.

Nella specie, si sottolinea il carattere transnazionale di questi crimini che colpiscono la società e l'economia di tutti gli Stati, rendendo indispensabile la cooperazione internazionale.

La relazione russa si sofferma specificamente sull'importanza dell'assistenza tecnica, nel rafforzamento delle capacità di prevenzione degli Stati e nell'aumento del livello di sicurezza delle informazioni.

La premessa fondamentale da cui origina la relazione dei rappresentanti russi è la tutela della sovranità. Gli Stati parte dovrebbero adempiere ai loro obblighi ai sensi della nuova Convenzione in conformità ai principi di sovranità dei paesi e di non ingerenza negli affari interni di altri Stati. La Convenzione non dovrebbe permettere alle autorità di uno Stato parte di esercitare nel territorio di un altro Stato la giurisdizione e le altre funzioni riservate esclusivamente al primo ai sensi del suo diritto interno.

Esaminando le disposizioni di diritto sostanziale inserite nel "progetto di convenzione" proposto dalla Russia, emerge subito la varietà delle fattispecie penali considerate. Si fa riferimento, in primo luogo, all'accesso non autorizzato alle informazioni o ai dati personali, alle intercettazioni non autorizzate, all'interferenza o interruzione di reti di informazione e comunicazione. Un articolo a parte è dedicato alla creazione, utilizzazione e distribuzione di *software* dannosi, ed al traffico non autorizzato di dispositivi, condotte che minano la sicurezza della rete internet. Particolare attenzione è riservata anche ai furti legati alle tecnologie informatiche.

Ma maggiormente articolata appare soprattutto la disciplina dei reati informatici legati alla tutela dei soggetti vulnerabili, come i minori o le persone in condizioni di fragilità psicologica. All'uopo, l'art. 15 disciplina la produzione e distribuzione di materiali o oggetti con immagini pornografiche di minori. Ciascuno Stato dovrebbe adottare misure legislative ed extralegislative per contrastare, ai sensi del proprio diritto interno, le condotte di produzione di materiale pedopornografico ai fini della diffusione nelle reti telematiche, compresa Internet; le condotte di offerta o messa a disposizione di materiale pedopornografico; la distribuzione, la trasmissione e la detenzione di materiale pedopornografico in un sistema informatico o su dispositivi elettronici per l'archiviazione di dati digitali. Nel termine "pedopornografia" si include il materiale pornografico che ritrae visivamente: a) un minore dedito a comportamenti sessualmente espliciti; b) una persona che sembri essere un minore impegnato in attività sessualmente esplicite; c) immagini realistiche che rappresentino un minore impegnato in attività sessualmente esplicite. Il termine "minore" comprende tutte le persone sotto i 18 anni di età. Gli Stati parte potrebbero, tuttavia, prevedere un diverso limite di età, che non dovrebbe essere inferiore a 16 anni.

L'articolo 17 dello schema contenuto nella relazione menziona poi il coinvolgimento di minori nella commissione di atti illeciti che mettono in pericolo la loro vita o la loro salute. A tal fine, si afferma l'obbligo di ciascuno Stato di adottare ogni misura per incriminare il coinvolgimento di minori attraverso l'uso di tecnologie informatiche nella commissione di atti illeciti potenzialmente letali.

A completamento di questo "microsistema" a tutela della persona contro l'uso delle tecnologie informatiche, il precedente articolo 16 disciplina l'istigazione o coercizione al suicidio. Come è tristemente noto, si tratta di reati gravissimi che spesso trovano nella rete un agevole veicolo di diffusione. A tal riguardo, si afferma l'obbligo degli Stati parte di punire ai sensi del proprio diritto interno l'incoraggiamento o la coercizione al suicidio, anche di minori, attraverso la motivazione psicologica o altra forma di pressione sulle reti di informazione e telecomunicazioni, compresa Internet. Sebbene simili condotte risultino oggi punibili in astratto nei principali ordinamenti europei, tra cui l'Italia, indubbiamente questa previsione potrebbe rappresentare un

adeguato minimo comune denominatore per gli Stati partecipanti alla Convenzione, come alcune realtà extraeuropee meno attente alle potenzialità criminogene delle reti.

Gli articoli 19, 20 e 21 sono, invece, dedicati ai reati connessi al terrorismo ed all'estremismo, che sono oggi favoriti dall'anonimato e dalla facilità di comunicazione offerta dalla rete. Nella specie, l'articolo 19 prevede l'incitamento ad attività sovversive o armate, mentre l'articolo 20, con una formulazione abbastanza generica, parla di reati connessi al terrorismo; l'articolo 21, infine, utilizza il diverso termine di "estremismo", a segnalare la necessità di contrastare la vasta gamma di reati caratterizzati da finalità sovversive o animati dall'odio. Sulla stessa linea, l'articolo 24 della proposta presentata dalla Russia cita anche i crimini di riabilitazione del nazismo, di giustificazione dei genocidi o i crimini contro la pace. In generale, l'estrema varietà di fattispecie citate mostra la consapevolezza della capacità diffusiva del cyberspazio rispetto a ideologie disumane e antidemocratiche.

Accanto a tali fattispecie, sono inclusi i principali traffici illeciti delle organizzazioni criminali su base transnazionale. L'articolo 22 disciplina i reati connessi allo spaccio di sostanze stupefacenti e l'articolo 23 i reati connessi al traffico di armi ed esseri umani. Riconoscere il legame essenziale intercorrente tra i principali *business* criminali e il cybercrime costituirebbe indubbiamente un aspetto innovativo della futura Convenzione.

Ancora, l'articolo 26 fa riferimento all'uso delle tecnologie cibernetiche nei rapporti tra gli Stati per commettere atti considerati reati dal diritto internazionale. Quest'ultima tematica si preannuncia particolarmente divisiva, essendo uno dei principali nodi da sciogliere nel contesto internazionale; lo sviluppo tecnologico e della rete ha portato infatti ad una politica generale di reciproca sorveglianza e cyberspionaggio che alcuni Stati avrebbero interesse a mantenere libera da stringenti regolamentazioni giuridiche. Sul punto, l'art. 26 afferma che ciascuno Stato parte adotta le misure necessarie per reprimere l'uso di strumenti informatici per commettere atti previsti come reato dagli accordi internazionali.

Con una formula di chiusura, il successivo articolo 29 statuisce che resta ferma la possibilità per ogni Stato parte della Convenzione di sanzionare qualsiasi condotta illecita, non rientrante nella Convenzione, commessa attraverso l'uso intenzionale di mezzi tecnologici e che provochi danni significativi.

Uno degli aspetti più rilevanti della proposta russa è rappresentato dall'auspicata inclusione nella futura Convenzione di adeguate forme di responsabilità delle persone giuridiche, non solo perché si riconosce il ruolo determinante degli organismi aziendali nelle strategie dei gruppi criminali, ma perché tale previsione si salderebbe idealmente con quanto già prevede l'art. 10 della citata Convenzione di Palermo.

Entrando nel dettaglio, l'articolo 30 del progetto russo impone agli Stati di adottare misure di responsabilità delle persone giuridiche per gli illeciti che saranno previsti dalla Convenzione, quando ricorre il requisito fondamentale della commissione a loro vantaggio da parte di qualsiasi persona fisica, che agisce individualmente o come parte dell'ente. In tal senso, si richiede che l'autore del reato ricopra una posizione apicale in virtù dell'attribuzione del potere di rappresentanza, del potere decisionale o

del potere di controllo all'interno dell'azienda. L'ente risponde anche se la mancanza di vigilanza o controllo da parte di una persona fisica con posizione apicale abbia reso possibile la commissione di un reato previsto dalla Convenzione da parte di una persona fisica che agisca sotto le direttive ed a beneficio di tale persona giuridica. Inoltre, si afferma che, fatti salvi i principi giuridici dello Stato parte, la responsabilità della persona giuridica può essere penale, civile o amministrativa, e che le sanzioni, anche quelle pecuniarie, devono essere effettive, proporzionate e dissuasive. Infine, la responsabilità dell'ente non pregiudica la responsabilità delle persone fisiche autrici del reato presupposto. Questa formulazione riecheggia chiaramente l'art. 10 della Convenzione di Palermo contro il crimine organizzato transnazionale, nella misura in cui, optando per un doppio binario di responsabilità, richiede una tutela effettiva a prescindere dal regime formale adottato dagli Stati parte.

*4.5. (*segue*) La Cina.*

La relazione presentata dalla Cina si concentra sul tema della prevenzione come principio primario. In tal senso, si afferma la necessità di definire le responsabilità delle istituzioni pubbliche e dei soggetti privati nella prevenzione della criminalità. Sotto questo profilo, gli Stati dovrebbero formulare misure mirate di prevenzione della criminalità incoraggiando al contempo la partecipazione della società civile e la cooperazione tra il settore pubblico e quello privato. In primo luogo, si suggerisce l'istituzione di agenzie specializzate per lo sviluppo di politiche di prevenzione e di monitoraggio del *cybercrime*. A tal fine, nell'adozione delle misure di sicurezza, occorrerebbe tenere conto delle caratteristiche delle strutture da proteggere. Nel settore privato, tali precauzioni possono includere programmi di sicurezza e di emergenza per incidenti della rete, gestione di virus informatici e intrusioni in rete, conservazione delle informazioni registrate. Nel determinare le responsabilità dei fornitori di servizi di rete, deve osservarsi un principio di proporzionalità, tenendo conto delle differenze nelle capacità dei fornitori di servizi di rete di diverse dimensioni.

In generale, secondo i rappresentanti cinesi, la futura Convenzione dovrebbe, sulla base dello sviluppo attuale e futuro delle tecnologie e delle esigenze di contrasto al crimine, fornire una base giuridica flessibile.

In relazione alle fattispecie sanzionabili, si fa riferimento all'intrusione ed alla distruzione di strutture, sistemi, dati o infrastrutture di informazioni critiche. Ciò può includere l'accesso illegale ai sistemi informatici, l'interferenza illecita con i sistemi informatici, l'acquisizione illegale di dati informatici, o la violazione di infrastrutture informatiche critiche. Secondo la Cina, nella Convenzione dovrebbero includersi anche le attività criminali solo agevolate dalle tecnologie informatiche, tra cui estorsioni, frodi informatiche, pornografia e pedopornografia, violazioni del diritto d'autore, incitamento e realizzazione di atti di terrorismo. In considerazione della crescente "industrializzazione" del *cybercrime*, dovrebbe essere inclusa nell'ambito della criminalizzazione tutta la "catena" delle operazioni illecite, compresi gli aiuti e gli atti preparatori, come lo sviluppo, la vendita e la diffusione di programmi e dati per la

criminalità. Per quanto riguarda le "prove elettroniche", dovrebbe essere regolata l'identificazione delle prove di natura elettronica nei procedimenti giudiziari, comprese le modalità per identificarne l'autenticità, l'integrità e la pertinenza.

Inoltre, data la particolarità del cyberspazio, si consiglia di fornire standard guida su come determinare la giurisdizione ed evitare conflitti di giurisdizione. La giurisdizione dovrebbe basarsi su un legame effettivo con la realizzazione del reato, prediligendo, tra gli altri, il luogo in cui si verifica l'evento del reato, il luogo in cui viene commesso il reato e quello in cui si trova l'autore.

Due aspetti centrali della posizione espressa dai rappresentanti cinesi riguardano la cooperazione internazionale e l'impegno di assistenza tecnica e formazione reciproca. L'anonimato e l'*intelligence* delle attività criminali, insieme alla rapidità di occultamento delle prove elettroniche, rappresentano una grande sfida per i meccanismi di cooperazione internazionale. La raccolta di prove elettroniche transfrontaliere è necessaria per combattere l'uso della rete a fini criminali, ma nel far ciò gli Stati membri dovrebbero rispettare la sovranità dello Stato in cui si trovano le prove. Non dovrebbero quindi essere raccolti i dati conservati in Stati esteri da imprese o singoli individui o con mezzi tecnici eludendo le misure di protezione della rete, se ciò sia contrario alle leggi dello Stato estero. Ancora, nell'adottare mezzi di indagine tecnici e particolarmente invasivi, gli Stati membri dovrebbero attenersi ai principi del giusto processo e rispettare gli altri diritti fondamentali dei soggetti coinvolti. Su un diverso fronte, si auspica l'introduzione di misure di confisca e sequestro dei proventi dei reati informatici ed il rafforzamento della cooperazione internazionale in una logica di rapida ed efficace ablazione dei profitti illeciti.

Ciò detto, la relazione cinese ritiene strategico il tema dell'assistenza tecnica e dello scambio di informazioni. Sotto tale profilo, è essenziale colmare le disparità di risorse fornendo assistenza tecnica ai paesi in via di sviluppo e rafforzando lo scambio di informazioni.

Questa assistenza tecnica dovrebbe includere la formazione degli operatori giudiziari e di polizia, l'istituzione di gruppi di esperti con competenze tecnico-legali, lo sviluppo delle tecniche di indagine elettronica, e la fornitura di attrezzature e tecnologie.

A prescindere dalle petizioni di principio, l'aspetto fondamentale riguarderà la politica effettivamente adottata dai paesi citati.

4.6. La sorveglianza elettronica: uno strumento di difficile inquadramento.

Come si è visto, nel contesto della nuova Convenzione un ruolo cruciale è attribuito dagli Stati partecipanti alle tecniche di sorveglianza elettronica. La nozione di "sorveglianza elettronica" è impiegata dall'art. 20 della Convenzione di Palermo e dall'art. 50 della Convenzione di Merida[42].

[42] Per un'analisi generale del tema, v. A. BALSAMO, *op. cit.*, p. 302 ss.

Gli studi condotti dall'UNODC[43] hanno sottolineato la particolare utilità e l'estrema ampiezza della categoria in esame, essendosi identificate 15 diverse tipologie, distinte a loro volta in quattro gruppi. Viene in rilievo, in primo luogo, l'audio-sorveglianza attraverso intercettazioni telefoniche (*phone-tapping*), il protocollo *Voice Over Internet* (VOIP) e le intercettazioni ambientali attraverso microspie (*room bugging*). In secondo luogo, l'UNODC cita la sorveglianza visiva, condotta attraverso dispositivi di videosorveglianza nascosti in immobili (*hidden video surveillance devices*), su automobili (*in-car video systems*), sulle persone (*body-worn video devices*), ovvero con termografia o rilevazione delle radiazioni infrarosse (*thermal imaging/forward looking infrared*), nonché con telecamere a circuito chiuso (CCTV). Ancora, le tecnologie odierne contemplano la sorveglianza mediante geolocalizzazione (*Global positioning systems - GPS/transponders*) o scansione della retina o delle altre informazioni biometriche (*biometric information technology*), utilizzata ad esempio negli aeroporti. Infine, la sorveglianza elettronica può sfruttare il monitoraggio delle celle utilizzate dai telefoni cellulari (*mobile phones*) o i dispositivi di identificazione a radiofrequenza (*Radio frequency identification devices-RFID*).

Ai fini della presente trattazione, vanno menzionate soprattutto le più innovative forme di sorveglianza sui dati, come gli *spyware* e i *cookies* utilizzati sui computer e su Internet, insieme alle altre tecniche utilizzate sui telefoni cellulari, come il *keystroke monitoring*.

Pertanto, nella nozione di "sorveglianza elettronica" rientrano tutti i nuovi strumenti investigativi, come il c.d. "captatore informatico"[44], che, servendosi di meccanismo tecnologici, producono, di fatto, gli stessi effetti di una pluralità di altri mezzi di ricerca della prova, sia tipici che atipici, come le intercettazioni telefoniche, ambientali[45], di comunicazioni informatiche o telematiche, la perquisizione di un sistema

---

[43] UNODC, *Current practices in electronic surveillance in the investigation of serious and organized crime*, United Nations, New York, 2009, p. 2.

[44] In proposito va segnalato che, tutte le volte in cui si parla di "captatore informatico" in ambito investigativo è necessario distinguere tra due diverse modalità operative: la *on line search* e la *on line surveillance*. I programmi appartenenti alla categoria della *on line search* (modalità acquisitiva di dati) consentono di far copia, totale o parziale, delle unità di memoria del sistema informatico individuato come obiettivo; i dati e le informazioni sono quindi trasmessi, in tempo reale o ad intervalli prestabiliti, agli organi di investigazione tramite la rete Internet in modalità nascosta e protetta. Attraverso i programmi che realizzano la *on line surveillance* (modalità captativa di flussi informativi) invece, è possibile captare il flusso informativo intercorrente tra le periferiche (video, tastiera, microfono, webcam, ecc.) e il microprocessore del dispositivo *target*, consentendo al centro remoto di controllo di monitorare in tempo reale tutto ciò che viene visualizzato sullo schermo (*screenshot)*, digitato attraverso la tastiera (*keylogger*), detto attraverso il microfono, o visto tramite la webcam del sistema target controllato. Al riguardo v. M. TORRE, *Il virus di Stato nel diritto vivente tra esigenza investigative e tutela dei diritti fondamentali*, in *Diritto Penale e Processo*, 2015, 1163 ss., nonché A. BALSAMO – A. LO PIPARO, *Prova*, in *Processo di criminalità organizzata*, nel *Codice di Procedura Penale Commentato* a cura di A. GIARDA - G. SPANGHER, Tomo III, Wolters Kluwer, Milano, 2017.

[45] L'effetto captativo, peraltro, si esplica nei confronti di una cerchia di soggetti potenzialmente indeterminata, costituita da tutti coloro che ricadono nel raggio di azione del dispositivo "infettato" dal *trojan*. Si tratta, infatti, di captazioni che possono definirsi come "intercettazioni ambientali mobili", in contrapposizione a quelle "statiche" ottenute con il mezzo tradizionale delle microspie collocate all'interno di uno specifico immobile o mezzo di trasporto. Le nuove forme di captazione, invece, consentono di

informatico o telematico, il sequestro di dati informatici, le videoriprese[46]. L'esempio tipico è rappresentato dai programmi *trojan horse* installati riservatamente su dispositivi elettronici come *personal computer*, *tablet* o *smartphone*[47].

Gli strumenti citati sono oggi fondamentali di fronte all'evoluzione del sistema globale delle comunicazioni, dipendenti in larga parte da sistemi telematici, a cui corrisponde una nuova strategia delle organizzazioni criminali, fondata sull'uso della tecnologia informatica anche per i reati soltanto cyber-correlati e non legati in senso stretto al *cybercrime*. Sul punto, è sufficiente rammentare, per citare i casi principali, come l'azione e la propaganda dei terroristi, il traffico internazionali della droga, il commercio illecito di beni culturali e il riciclaggio di denaro sporco siano basati oggi essenzialmente sulle comunicazioni effettuate attraverso la rete Internet. Sotto tale profilo, le nuove tecnologie di indagine[48], che rientrano nella sorveglianza elettronica consentono di superare gli ostacoli che incontrano le intercettazioni tradizionali, rappresentati dai sistemi di criptazione delle comunicazioni di cui si servono i programmi utilizzati ogni giorno da milioni di persone.

Peraltro, in mancanza di una base giuridica adeguata che ne consenta l'impiego su obiettivi situati all'estero, e senza un'indispensabile opera di armonizzazione degli ordinamenti, che eviti la creazione di zone franche, la sorveglianza elettronica rischia di divenire un'arma spuntata. L'attività investigativa rischia di essere imbrigliata nei

---

raggiungere non solo l'individuo nelle più diverse manifestazioni della sua vita, ma anche i soggetti a lui vicini, senza alcun limite relativo ai luoghi di ascolto. V. sul punto A. BALSAMO – A. LO PIPARO, *Prova*, cit.

[46] Si tratta di *software* che acquisiscono determinati poteri di gestione di un sistema scelto come "obiettivo" (sia esso un *personal computer*, un *tablet* od uno *smartphone*), funzionando come una sorta di microspia telematica. Nelle versioni più evolute questi software possono operare come veri e propri sistemi di controllo remoto (RCS: *remote control systems*), e funzionare in modo autonomo, senza l'intervento diretto di persone responsabili. Sul punto v. A. TESTAGUZZA, *I sistemi di controllo remoto: fra normativa e prassi*, in *Diritto Penale e Processo*, 2014, p. 759 ss., nonché A. BALSAMO – A. LO PIPARO, *Prova*, cit.

[47] L'installazione del software sul sistema *obiettivo* (la c.d. "inoculazione") all'insaputa del suo possessore può essere compiuta o mediante un accesso fisico al computer obiettivo o grazie ad installazione remota (attraverso l'invio di allegati con messaggi di posta elettronica o l'invio di comunicazioni provenienti da gestori dei servizi di messaggistica o *social network* o l'invio di aggiornamenti di software o di applicazioni). Sul punto v. A. TESTAGUZZA, *Digital forensics. Informatica giuridica e processo penale*, Cedam, Padova, 2014, p. 81 ss., nonché A. BALSAMO – A. LO PIPARO, *Prova*, cit.

[48] Come la dottrina ha sottolineato, per intercettare le comunicazioni realizzate attraverso l'impiego di apparati mobili collegati a reti WI-FI "aperte" o effettuate da utilizzatori di sistemi crittografati, è necessario avvalersi di un modello diverso dalle intercettazioni telematiche "classiche", fondate sulla assistenza tecnologica degli operatori che forniscono un accesso alla rete e dirette alla acquisizione dei soli dati che vi fluiscano "in chiaro". Il *software trojan* si occupa della captazione della voce dell'utilizzatore e di quella dell'interlocutore dopo esser stata decifrata. Le informazioni così ottenute vengono mandate a *server* esterni, collocati presso la sala di ascolto. Ovviamente, questo avviene sfruttando la connettività del dispositivo elettronico scelto come *"obiettivo"*: laddove questo non abbia connettività, infatti, le informazioni verranno salvate in locale ed inviate al *server* non appena risulti disponibile un collegamento alla rete. In sostanza tali *software* catturano quanto captato dal microfono e, conseguentemente, ogni qualvolta il computer risulti acceso con i microfoni attivati, potrà realizzarsi una vera e propria, intercettazione "ambientale". In proposito v. A. TESTAGUZZA, *Digital forensics.*, cit., p. 81 ss., nonché A. BALSAMO – A. LO PIPARO, *Prova*, cit.

confini nazionali, senza poter frenare quindi la estrema mobilità che caratterizza, di contro, i traffici illeciti[49].

Le nuove forme di indagine che la tecnologia mette a disposizione, tra cui la sorveglianza elettronica, possono essere pienamente sfruttate contro il crimine organizzato transnazionale se utilizzate in sinergia con altri strumenti, come l'assistenza giudiziaria reciproca e le *Joint investigations*, previsti dagli artt. 18 e 19 della Convenzione di Palermo.

Al riguardo, è molto significativa la previsione nel secondo paragrafo dell'art. 20 della Convenzione di Palermo, che incoraggia gli Stati parte a concludere accordi o intese bilaterali o multilaterali per l'impiego delle tecniche speciali di investigazione nel contesto della cooperazione internazionale, nel debito rispetto del principio di uguaglianza sovrana degli Stati. Le tecniche di sorveglianza elettronica devono dunque essere inserite nel più ampio quadro della cooperazione giudiziaria internazionale e delle indagini comuni, in modo da rafforzare il contrasto a tutte le condotte di utilizzazione illecita dei sistemi di comunicazione che risultano impermeabili alle tradizionali forme di captazione.

Ciò richiede, però, un netto potenziamento dello scambio di informazioni, dell'assistenza tecnica, della cooperazione giudiziaria e di polizia. Un ruolo di impulso verso questo obiettivo può essere svolto dal Meccanismo di Revisione della Convenzione di Palermo, che si concentra sulla possibilità di ricorrere alle forme di sorveglianza elettronica nell'ambito di indagini comuni condotte da più Stati.

Un importante passo avanti nella stessa direzione è stato compiuto con riferimento alla Convenzione di Merida, con l'approvazione, da parte della Conferenza degli Stati parte, della risoluzione 8/6, che incoraggia la conclusione di accordi bilaterali e plurilaterali per l'uso di tecniche investigative speciali nella cooperazione internazionale finalizzata alle indagini su condotte di corruzione di natura transnazionale.

Questa strategia dovrebbe essere adottata anche nel contrasto al cybercrime, sia in occasione dell'implementazione delle Convenzioni già in vigore, sia con riferimento alla nuova Convenzione delle Nazioni Unite contro l'uso delle tecnologie per scopi criminali. Una regolamentazione unitaria è necessaria non solo per una più efficace repressione dei reati informatici, ma anche per garantire una tutela dei diritti omogenea tra i diversi ordinamenti, considerato l'alto potenziale intrusivo degli strumenti citati nella sfera privata dei cittadini.

5. Conclusioni: i possibili scenari e l'esigenza di tutelare i diritti fondamentali.

Nel loro insieme, le relazioni presentate dagli Stati partecipanti hanno rivelato alcuni ostacoli politici, ideologici e sostanziali alla creazione di un nuovo trattato sulla criminalità informatica.

---

[49] A. BALSAMO, *op. cit.*, p. 306.

In un'epoca in cui il cyberspazio è oggetto di contesa, il multilateralismo fatica a costruire fiducia tra i paesi. Data la mancanza di trasparenza che caratterizza l'opera di alcuni Stati nella lotta agli attacchi informatici, ci si è chiesti se essi vogliano realmente una convenzione che rischierebbe di evidenziare e punire determinate pratiche. Tuttavia, la gamma di minacce rivolte agli Stati ed ai cittadini induce a prefigurare un positivo esito degli sforzi messi in campo per la creazione di questo nuovo strumento normativo.

Occorre comunque scongiurare il pericolo che i nuovi strumenti possano essere utilizzati per comprimere i diritti umani e la libertà di espressione. Nel settore privato, le nuove disposizioni potrebbero rendere più facile prevenire e controllare attività *online* illegali, ma allo stesso tempo è necessario garantire la fiducia degli operatori nel sistema.

Le discussioni sul crimine informatico hanno visto contrapporsi due poli, ossia l'Europa occidentale e l'asse formato dalla Cina, dalla Russia e da alcuni Stati dell'Est Europa, con in testa l'Ungheria. Come si è visto, la Russia ha presentato una bozza di convenzione, mentre la Convenzione di Budapest sarà considerata lo standard dai paesi dell'Europa occidentale e potenzialmente anche da altri Stati membri.

Dati questi due poli, secondo alcuni commentatori[50], si delineano quattro possibili scenari per l'esito dei negoziati.

In primo luogo, si può ipotizzare che la convenzione sia in linea con la bozza russa. Nel corso degli anni, le proposte della Russia si sono avvicinate al contenuto della Convenzione di Budapest. Ma rimangono alcune perplessità degli Stati, essendo improbabile che una convenzione con una visione restrittiva in tema di sovranità digitale, proprietà dei dati e diritti umani venga adottata a maggioranza e non finalizzata tramite il metodo del *consensus*, sebbene durante tutto il processo sia richiesta una maggioranza di due terzi. Un simile scenario accrescerebbe il ruolo della Russia e della Cina nello sviluppo delle capacità di contrasto al *cybercrime* tra i firmatari, ma non farebbe molto per facilitare la cooperazione internazionale. L'adozione di una convenzione guidata dalla Russia è stata vista da alcuni commentatori come un possibile passo indietro per i diritti umani e la libertà di espressione *online* e una sfida per le aziende internazionali che operano nei paesi che la adottano.

In secondo luogo, si potrebbe prospettare una soluzione di mediazione. La previsione di una maggioranza dei due terzi si presta a questa conclusione, che porterebbe a soluzioni comuni sulla terminologia adottata, lasciando un maggiore spazio all'interpretazione da parte delle autorità nazionali. Tutto ciò consentirebbe probabilmente un'adesione diffusa, così come è avvenuto per la Convenzione delle Nazioni Unite di Palermo contro il crimine organizzato transnazionale, che è adottata quasi universalmente, in virtù della sua flessibilità. Ciò potrebbe fornire una guida per la criminalizzazione e creare nuovi orientamenti per la cooperazione internazionale. Inoltre, potrebbe anche qui prevedersi un meccanismo di revisione per aumentare la trasparenza generale nella cooperazione nella lotta alla criminalità informatica e per il monitoraggio dell'attuazione e della comprensione del suo impatto.

---

[50] S. WALKER - I. TENNANT, *Control, Alt, or Delete? The Un cyber crime debate enters a new phase*, cit., p. 24.

Un terzo scenario è rappresentato da una sostanziale riproposizione, ad un livello più esteso, della Convenzione di Budapest. Un trattato di tale contenuto accrescerebbe l'adesione ai valori del Consiglio d'Europa, conferendo a quel quadro normativo il sigillo delle Nazioni Unite. Anche in questa ipotesi, non si avrebbe un aumento della cooperazione internazionale, data la mancata adesione di alcune grandi potenze. Si potrebbe eventualmente rafforzare la cooperazione tra l'Occidente e i nuovi Stati firmatari. Lo scenario tracciato innalzerebbe gli standard di tutela diritti umani e sarebbe maggiormente accettabile anche per il settore privato, che sta già lavorando con le disposizioni di Budapest.

Infine, è possibile che i negoziati siano talmente paralizzati dai veti incrociati da non ottenere alcun risultato. Ciò rappresenterebbe un fallimento per il multilateralismo, e lascerebbe frammentata la cooperazione internazionale sulla lotta alla criminalità informatica.

In conclusione, le sfide imposte dalla rivoluzione digitale rappresentano un importante banco di prova per il penalista. Se il crimine organizzato transnazionale negli ultimi decenni ha esteso l'ambito spaziale del contrasto ai reati, il *cybercrime* invece sposta la contesa su un universo radicalmente alternativo, retto da regole diverse e privo dei riferimenti spaziali e temporali di cui il diritto penale tradizionalmente si nutre[51]. Di fronte ad una criminalità dematerializzata e senza confini geografici, in grado di colpire dovunque nel mondo e in qualunque momento, viene portata all'estremo l'esigenza di internazionalizzazione della prevenzione e repressione dei reati.

Gli aspetti principali con cui la nuova Convenzione delle Nazioni Unite dovrà confrontarsi sono quelli dell'armonizzazione degli ordinamenti e della specializzazione degli operatori. In tal senso, è indispensabile elevare gli standard di tutela a livello internazionale, per evitare che si creino "zone franche" esposte agli attacchi *hacker*. Soprattutto, è urgente provvedere alla formazione di una cultura della *cybersecurity* in tutti gli operatori giuridici e nelle realtà aziendali, in quanto alla dirompente espansione degli strumenti telematici non è corrisposta una adeguata consapevolezza dei rischi criminogeni derivanti dalla rete[52].

Infine, tutti gli Stati partecipanti al futuro strumento giuridico hanno auspicato che il contrasto al *cybercrime* avvenga nel rispetto dei diritti fondamentali, nell'ambito di un bilanciamento degli interessi in gioco, come la sicurezza, da una parte, e la privacy e la libertà personale e di comunicazione, dall'altra. Come si è visto, infatti, alla pervasività dei reati informatici corrisponde una notevole incidenza delle tecniche di indagine nella sfera privata dei cittadini[53]. Il non facile compito degli Stati sarà allora il raggiungimento di un adeguato equilibrio, per evitare che il contrasto alle nuove forme di criminalità vanifichi le conquiste e le possibilità, anche in termini di libertà, offerte dal cyberspazio.

---

[51] Una riflessione recente si deve a L. PICOTTI, *Cybersecurity: quid novi?*, in *Dir. Internet*, 2020, pp. 13 ss.

[52] Per un approfondimento sull'importanza della *compliance* aziendale nell'ambito dei reati informatici, *ex multis*, V. DEZZANI-PICCINNI, *Gli strumenti di sorveglianza aziendali per la prevenzione dei crimini informatici quali reati presupposto nell'ambito di applicazione del D.lgs. 231/2001*, in *Resp. amm. Soc. ed enti*, n. 2/2011.

[53] In tema di captatore informatico e virus trojan, M. TORRE, *op. cit.*