SPAZIO VIRTUALE

LE GARANZIE DI GIURISDIZIONE NELLA RESILIENZA E NELLA DIFESA DELLA SICUREZZA NAZIONALE

ROMA - Palazzo della Farnesina

11-12 Ottobre 2024

Atti del convegno

Quaderno della Rivista Trimestrale
della Scuola di Perfezionamento per le Forze di Polizia

I 2025

Il seminario è stato organizzato unitamente alla Presidenza del Consiglio dei Ministri, ai Ministeri degli Affari Esteri e della Cooperazione Internazionale, dell'Interno e della Giustizia, all'Agenzia per la Cybersicurezza Nazionale e al Dipartimento delle Informazioni per la Sicurezza.

Si ringraziano per il prezioso contributo Acea, l'Agenzia delle Entrate, la Camera di Commercio, Coldiretti, e l'Osservatorio Agromafie.

Si ringrazia, in particolare,

il dott. Andrea Apollonio,
Sostituto Procuratore presso il Tribunale di Patti,

l'avv. Andrea Daranghi
di Agenzia delle Entrate,

la dott.ssa Carola Desideri
di Acea,

la dott.ssa Tiziana Leone
della Presidenza del Consiglio dei Ministri,

la dott.ssa Simona Ragazzi,
GIP presso il Tribunale di Catania

e il team della Fondazione Vittorio Occorsio,
coordinato dalla dott.ssa Jasmin Petti
e composto dal dott. Joseph Omari e dal dott. Filippo Iacomini.

L'accoglienza è stata curata
dagli allievi dell'Istituto Superiore Alberghiero
"Francesco Morano" di Caivano (NA).

INDICE - SOMMARIO

PREFAZIONI

Maurizio Vallone
Direttore della Scuola di Perfezionamento per le Forze di Polizia

La Scuola di Perfezionamento per le Forze di Polizia, ormai da diversi anni, in collaborazione con la Fondazione Vittorio Occorsio, affronta i temi delle nuove frontiere tecnologiche, le quali offrono innovative opportunità alle Forze di Polizia per un più efficace contrasto al crimine organizzato, al terrorismo internazionale ed alla criminalità economica. Le stesse tecnologie che, d'altra parte, vengono ormai largamente utilizzate dal mondo criminale per rendere non intercettabili le comunicazioni, non tracciabili i flussi finanziari, per creare nuove opportunità di affari illeciti ed aumentare così la capacità di consumare reati ed occultarne i profitti.

Lo sforzo della Scuola e della Fondazione Occorsio è quello di consentire, sia ai frequentatori dei Corsi di Alta Formazione sia ai partecipanti ai convegni, come quello dello scorso 11 e 12 ottobre 2024 oggetto della presente pubblicazione, di acquisire la migliore conoscenza, giuridica e tecnica, del mondo digitale, laddove la tecnologia è ormai inscindibile dalle tecniche investigative ed è per esse imprescindibile: dunque non può più essere confinata alla conoscenza ed attività di esperti specialisti bensì deve costituire patrimonio comune degli investigatori e di chi è chiamato a dirigere uffici investigativi o di coordinamento investigativo.

In quest'ambito, viene sempre più affrontato il tema dell'Intelligenza Artificiale e delle sue applicazioni al mondo dell'intelligence e del crimine, tema di stretta attualità giuridica ed operativa, ma che dovrebbe essere valutato in una ottica evolutiva e prospettica, evitando di "ingabbiarlo" in frettolose definizioni giuridiche che la tecnologia, nel volgere di pochi mesi, potrà agevolmente rendere obsolete e non più rispondenti ai nuovi canoni tecnici.

In effetti, l'intelligenza artificiale viene definita dall'IA Act dell'Unione Europea (art. 3) come *"un sistema automatizzato (basato su macchine) progettato per funzionare con diversi livelli di autonomia e che può mostrare capacità di adattamento dopo l'installazione e che, per obiettivi espliciti o impliciti, deduce, dagli input che riceve, come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali*".

Appare assolutamente chiaro come la visione del legislatore europeo è basata sui soli esempi ad oggi noti di AI, come le applicazioni per testi tipo Chat GPT.

In realtà, una definizione scientifica di Intelligenza Artificiale non esiste dal punto di vista informatico: il termine AI viene usato semplicemente come sinonimo di software, cioè un programma per computer capace di generare output a fronte di un input. Ma tutti i programmi software hanno fatto, da sempre, esattamente questo.

Anche una semplice addizione non è altro che un input (procedi alla somma di 2 + 2) il cui risultato (output) è la generazione di un dato nuovo (il 4).

Anche le aspettative circa la capacità adattiva o generativa dell'AI restano, al momento, affascinanti suggestioni: i programmi informatici, anche i più sofisticati, fanno solo ed esattamente quanto gli viene richiesto e, anche quando generano un prodotto prima non esistente, fanno ciò sulla base di un preciso programma e secondo le logiche che vi sono imposte (algoritmo).

Non può essere considerato generativo il prodotto di un software che fornisce un esito argomentato acquisendo dal web tutto ciò che trova sulla domanda che gli è posta, e che ordina gli esiti della ricerca secondo sequenze logiche probabilistiche (se 10 fonti dicono che il cavallo di Napoleone era bianco, è plausibile che lo fosse davvero, quindi l'AI mi dirà che il cavallo di Napoleone era bianco).

Se così è, governare l'AI significa regolamentare le informazioni concretamente fruibili al software, onde essere sicuri che il prodotto esitato sia accettabilmente verificato.

Infatti, se l'ambito di ricerca delle informazioni è quello del mio dominio informatico (il mio PC, la mia rete domestica o professionale, l'insieme dei domini dei quali conosco i processi di alimentazione informativa), posso essere sicuro che l'output mi fornirà un prodotto "pulito" e "verificato".

Viceversa, se la fonte delle informazioni ricercate dal software è il web, se non addirittura il dark web, ed il sistema è in grado di rilevare e sistematizzare da solo le informazioni pescate in ambiti non verificati – ciò che accade oggi per i software di AI - allora l'output non potrà definirsi certificato, perché il processo deduttivo potrà essere condizionato da informazioni errate o volutamente artefatte presenti sul web.

Si pensi soltanto alle campagne denigratorie di personaggi famosi o di politici durante le campagne elettorali, tese proprio a screditare tali persone e a condizionare le competizioni elettorali.

Ciò vale a maggior ragione se si tratta di argomenti controversi dove, proprio nel web, si scatenano campagne di disinformazione ad opera di soggetti militanti molto attivi in ambito informatico (ad esempio i NO VAX o i cd. Terrapiattisti).

In definitiva, il fondamentale problema legato all'AI è quello della "au-

tenticazione delle fonti": di governare tali fonti da cui i software traggono le informazioni che poi analizzano per realizzare il prodotto finale da consegnare all'utente.

Sull'autenticazione delle fonti molto si discute e spesso alla fine si getta la spugna, per la estrema difficoltà di prevedere, nel mondo d'oggi, un sistema che possa effettivamente garantire che il prodotto finale si basi solo su fonti qualificate e certificate.

Chi è in grado di certificare i miliardi di informazioni che girano sul web? Ovviamente nessuno, neanche le più performanti delle macchine.

E poi: possiamo limitare lo sviluppo dell'AI? Possiamo richiedere ai produttori di certificare le loro fonti? E in quale ambito territoriale possiamo tentare di fare questo? L'Unione Europea è intervenuta con l'AI ACT. Ebbene, possiamo fondatamente ritenere che Paesi potenzialmente ostili (o anche solo economicamente competitivi) possano accettare restrizioni alle loro capacità digitali in nome di una "Democrazia informatica"?

Il tema delle regole in questo campo è un tema di grande rilievo per la competitività delle nostre aziende, della nostra difesa (il Generale Carmine Masiello, Capo di Stato Maggiore dell'esercito, ha rappresentato il pericolo che le limitazioni normative all'utilizzo dell'intelligenza artificiale in Europa ed in Italia possano indebolire la nostra capacità di evoluzione tecnologica nei campi della difesa e dell'intelligence militare nei confronti di soggetti stranieri potenzialmente ostili che invece non hanno analoghe limitazioni), della stessa Pubblica Amministrazione la quale, per essere efficace ed efficiente e rispondere alle sfide dei prossimi anni, deve necessariamente avvalersi di strumenti di AI estremamente performanti e capaci di costituire un ausilio di altissimo livello all'operatore nonché di supporto al decisore.

Accanto al tema della certificazione delle fonti, si pone l'imprescindibile rilievo dell'uso etico dell'IA.

Il tema assume tale rilevanza che la Presidenza italiana del G7 ha inserito questo argomento nell'agenda del summit dei Capi di Stato e di Governo dello scorso giugno in Puglia. Tale sessione è stata aperta, per la prima volta nella storia, a testimonianza dell'importanza dell'argomento, da Sua Santità Papa Francesco, che ha ricordato come "*è proprio dall'utilizzo di questo potenziale creativo che Dio ci ha donato che viene alla luce l'intelligenza artificiale. Quest'ultima, come è noto, è uno strumento estremamente potente, impiegato in tantissime aree dell'agire umano: dalla medicina al mondo del lavoro, dalla cultura all'ambito della comunicazione, dall'educazione alla politica. Ed è ora lecito ipotizzare che il suo uso influenzerà sempre di più il nostro modo di vivere, le nostre relazioni sociali e nel futuro persino la maniera in cui concepiamo la nostra identità di esseri umani*".

Il Santo Padre ci ricorda dunque la necessità di una comune radice etica nell'applicazione di qualsiasi strumento, sia esso informatico che manuale.

Ebbene, l'Ai Act si basa sul principio che l'IA deve essere sviluppata e utilizzata in modo sicuro, etico e rispettoso dei diritti fondamentali e dei valori europei. Per questo motivo, il regolamento prevede una classificazione dei sistemi di IA in base al loro livello di rischio per la sicurezza e i diritti delle persone, e stabilisce una serie di requisiti e obblighi per i fornitori e gli utenti di tali sistemi. Dunque, L'AI non potrà mai essere utilizzata se non in conformità dei nostri principi costituzionali, e quindi mai per profilazioni razziali, sessuali, religiose etc. o per creare discriminazioni o aggravare condizioni di disagio sociale.

Giungiamo, quindi, non ad una generale certificazione di tutto quello che l'AI produce, ma ad un consapevole utilizzo di quel prodotto.

Possiamo e dobbiamo utilizzare l'AI per velocizzare i processi produttivi e razionalizzare le informazioni certificate già in nostro possesso, per porle alla base di decisioni che, come tali, saranno frutto di un maggiore contributo informativo, già razionalizzato ed organizzato, per consentire al decisore una più veloce "precedentazione" ed un supporto alla decisione finale che, se implica diritti di terzi, deve essere presa con la piena consapevolezza che le informazioni su cui poggia sono autentiche e frutto di una "umanizzazione" che solo l'intelletto e la professionalità di un essere umano può operare.

Vito Tenore (Presidente di Sezione della Corte dei Conti) ha recentemente pubblicato un saggio dal titolo *"Può l'AI sostituire il giudice?*". Ebbene, essa potrà farlo in Paesi dove la componente umana non ha rilievo nella decisione di una controversia. Certamente, ed in linea con l'autore, non potrà accadere in Italia dove, oltre alle recenti previsioni normative, il valore primario viene dato alla valutazione caso per caso che solo il Giudice può dare all'esito del processo.

Ovviamente l'AI può trovare largo impiego anche nel nostro sistema giudiziario, per sistematizzare gli atti, per ricercare con maggiore rapidità e completezza le massime della Cassazione, per cercare similitudini e precedenti nell'ormai ampio campo della giurisprudenza europea e delle Corti internazionali, atti questi tutti certificati, che possono essere efficacemente sintetizzati e posti all'attenzione del giudicante, che ne trarrà linfa per le proprie determinazioni.

Desidero ringraziare la Fondazione Occorsio per il grande ed efficace contributo che dà alla Scuola in tema di formazione su temi di grande complessità ed innovazione, ed in particolare il Procuratore Giovanni Salvi, tutti i membri del Comitato Scientifico, ed i relatori dei vari convegni.

Oreste Pollicino

Ordinario di diritto costituzionale, Università Bocconi e rappresentante italiano presso l'Agenzia europea per la protezione dei diritti fondamentali, Special Advisor Fondazione Vittorio Occorsio

Nell'era della digitalizzazione avanzata e dell'intelligenza artificiale di frontiera, il cyberspazio si configura come il nuovo teatro di confronto globale, dove disinformazione, attacchi informatici e manipolazioni algoritmiche minacciano non solo la sicurezza nazionale, ma anche la tenuta delle istituzioni democratiche. La giurisdizione, come sottolineato da Giovanni Salvi nella sua introduzione, non è solo un meccanismo di regolazione dei conflitti, ma un presidio imprescindibile della sovranità e della rule of law, chiamato oggi a rispondere a sfide di inedita complessità.

Le operazioni malevole nel cyberspazio si caratterizzano per una combinazione di opacità, transnazionalità e volatilità, elementi che mettono in crisi i tradizionali strumenti giuridici. La difficoltà di attribuire responsabilità, unita alla necessità di agire con rapidità, impone un ripensamento delle strategie normative e processuali. Non si tratta solo di individuare i responsabili di crimini informatici, ma di prevenire e mitigare i danni attraverso un coordinamento tra intelligence, giurisdizione e cooperazione internazionale.

Un tema centrale emerso durante il convegno è stato quello della regolamentazione della disinformazione come strumento di destabilizzazione politica e sociale. La manipolazione dell'informazione, amplificata da algoritmi di intelligenza artificiale sempre più sofisticati, rappresenta una minaccia sistemica. Come evidenziato da Salvi, la disinformazione non incide solo sulla fiducia pubblica, ma agisce direttamente sui processi decisionali democratici, richiedendo un intervento regolatorio multilivello. È in questo contesto che la co-regolamentazione si profila come una strategia particolarmente promettente, poiché mira a combinare la flessibilità dell'autorità privata con la garanzia di controllo pubblico.

A tal proposito, la nuova stagione regolatoria europea, incarnata dal Digital Services Act (DSA) e dall'Artificial Intelligence Act (AI Act), testimonia un significativo cambio di paradigma. La transizione dall'automazione algoritmica all'autonomia decisionale dell'intelligenza artificiale introduce infatti nuove sfide, soprattutto per quanto riguarda la tutela dei diritti fondamentali. Mentre la regolamentazione degli algoritmi di automazione si concentrava principalmente sull'affidabilità dei sistemi e sulla protezione dei dati, l'autonomia decisionale dell'IA richiede un controllo ancora più stringente, per garantire che i sistemi non operino in modo lesivo per i diritti individuali o collettivi.

La distinzione tra automazione e autonomia è cruciale: l'automazione riguarda processi meccanici o algoritmici che eseguono compiti secondo regole predeterminate, mentre l'autonomia implica la capacità di un sistema di apprendere, adattarsi e prendere decisioni in modo indipendente. Questo passaggio comporta, una necessaria evoluzione del quadro regolatorio verso un modello che integri principi di trasparenza, responsabilità e supervisione umana costante.

Un ulteriore elemento di rilievo è rappresentato dall'emergere di poteri privati digitali di natura quasi sovrana, capaci di influenzare il dibattito pubblico e di condizionare il funzionamento delle democrazie. La risposta giurisdizionale a tali poteri non può limitarsi alla semplice applicazione di norme preesistenti, ma deve essere proattiva e creativa, favorendo l'introduzione di nuovi strumenti di enforcement che garantiscano un effettivo bilanciamento tra innovazione e protezione dei diritti.

In questo senso, la co-regolazione si presenta come un modello particolarmente efficace. Essa prevede una collaborazione stretta tra autorità pubbliche e attori privati, con l'obiettivo di definire standard comuni e di assicurare il rispetto delle normative attraverso meccanismi di controllo condivisi. Tale approccio consente di superare le rigidità della regolazione tradizionale e di rispondere in modo più rapido e adeguato alle continue evoluzioni del contesto tecnologico.

La cooperazione internazionale è stata un ulteriore filo conduttore del convegno, evidenziando come nessun Paese possa affrontare da solo le sfide poste dal cyberspazio. Strumenti come il Secondo Protocollo Addizionale della Convenzione di Budapest e la futura Convenzione ONU sui crimini informatici rappresentano passi importanti verso un quadro normativo condiviso, ma restano ancora molte le questioni aperte. Salvi ha sottolineato l'importanza di sviluppare un consenso internazionale basato su valori comuni e sulla condivisione di buone pratiche, al fine di garantire una risposta coordinata ed efficace alle minacce digitali transnazionali.

Infine, il convegno ha posto in evidenza come la regolazione del cyberspazio e dell'intelligenza artificiale non possa prescindere da una prospettiva costituzionale. L'equilibrio tra innovazione e tutela dei diritti deve essere il principio guida di qualsiasi intervento regolatorio. Solo un approccio integrato, che coniughi sicurezza, cooperazione internazionale e salvaguardia dei diritti fondamentali, potrà garantire una resilienza istituzionale adeguata alle sfide del futuro.

INTRODUZIONE

Giovanni Salvi
già Procuratore generale presso la Suprema Corte di Cassazione, Presidente del Comitato Scientifico Fondazione Vittorio Occorsio

Dall'11 al 12 ottobre del 2024 si è tenuto nella sede del MAECI, Sala delle Conferenze Internazionali, Palazzo Farnesina, il seminario *Spazio Virtuale - Le garanzie della giurisdizione nella resilienza e nella difesa della sicurezza nazionale,* organizzato dalla Fondazione Vittorio Occorsio in collaborazione con la Presidenza del Consiglio dei ministri, nell'ambito del G7 a presidenza italiana.

I lavori sono stati introdotti da Vittorio Occorsio, a nome della Fondazione e del padre Eugenio, dal Vicepresidente del Comitato Scientifico Stefano Lucchini e dal Segretario Generale della Farnesina, Ambasciatore Riccardo Guariglia. Il Vicepresidente del CSM, Fabio Pinelli, la Presidente della Scuola Superiore della Magistratura, Presidente emerita della Corte Costituzionale, Silvana Sciarra, il Procuratore generale della Corte d'Appello di Roma, Giuseppe Amato, hanno contribuito con saluti non formali ma di ricco contenuto.

Il seminario ha visto la partecipazione dei Ministri Matteo Piantedosi e Carlo Nordio, del Sottosegretario Alfredo Mantovano – oltre ai saluti del Ministro Antonio Tajani – del Presidente del COPASIR, Lorenzo Guerini, e dei rappresentanti al più alto livello del Dipartimento delle Informazioni per la Sicurezza (DIS) - Vicedirettore Alessandra Guidi -, dell'Autorità Nazionale per la Cybersicurezza (ANC) - Direttore Bruno Frattasi e Vicedirettore Nunzia Ciardi -, della Corte di cassazione e delle Procure generali di cassazione e di appello, di esponenti della giurisdizione, delle istituzioni europee e italiane, di esperti internazionali.

La giornata di apertura è stata introdotta dalla relazione della prof.ssa Paola Severino e dalle relazioni tecniche della dr.ssa Keiko Kono e del Ten. Col. Massimiliano Signoretti.

I lavori sono proseguiti nelle tre sessioni sui temi specifici, presiedute dal Prefetto Alessandro Pansa, dal Segretario Generale della Corte di Cassazione, Stefano Mogini e dal Procuratore Generale della Corte di Cassazione, Luigi Salvato.

Le potenziali applicazioni delle nuove misure di cooperazione e i com-

plessi rapporti tra giurisdizione e Intelligence sono stati discussi da esperti di diritto pubblico internazionale. Tra questi, il vice presidente della Corte penale internazionale giudice Rosario Aitala, il prof. Marko Milanovic – attuale responsabile della elaborazione del Manuale Tallinn 3 del *NATO Center of Excellence* (CCDCOE)– il ten. Col. Massimiliano Signoretti – già esperto italiano nella redazione del Manuale Tallinn 2 – Danilo Ceccarelli, rappresentante della Procura Europea, il giudice Antonio Balsamo, esperto internazionale e già Presidente del Tribunale di Palermo, i professori Oreste Pollicino e Marco Roscini, tra i principali esperti di diritto internazionale, l'ambasciatore Denis Craig Wilder.

I rappresentanti italiani (Ministro Plenipotenziario Michele Giacomelli e Capo Dipartimento del Ministero della Giustizia Luigi Birritteri) e di altri Paesi e Istituzioni sovranazionali (L'Alto Inviato del Segretario generale delle Nazioni Unite per la Tecnologia, Amandeep Singh Gill, il rappresentante di UNODC Glen Prichard, l'Ambasciatrice degli Stati Uniti, Deborah Mc Carthy, e il rappresentante del Ministero degli Esteri brasiliano, Eric Do Val Lacerda Sogocio, entrambi vice presidenti dell'*Ad Hoc Committee on Cybercrime Convention*) hanno illustrato lo stato dei lavori *dello Open Ended Working Group on Security of and in the use of Information and Communication Technologies* delle Nazioni Unite (OEWG) sullo Spazio Virtuale e lo schema di Convenzione sul Cybercrime, definitivamente approvato dal Comitato.

Infine, esperti provenienti da diversi organismi giudiziari e di Law Enforcement (Polizia Postale e delle Telecomunicazioni, Eurojust e Europol) hanno discusso delle implicazioni delle nuove tecnologie sugli strumenti di indagine, in particolare con riferimento alle cripto-piattaforme; coordinati dal magistrato Eugenio Albamonte, hanno discusso il tema Ivano Gabrielli, Hannes Glantshnig e Edvardas Sileris.

All'interno della news del sito, è visibile il programma completo e il link alle dirette youtube delle due giornate della Conferenza:

https://www.fondazioneoccorsio.it/virtual-space/

Il Seminario è anche il frutto della cooperazione con la Scuola Interforze del Ministero dell'Interno. Il lavoro comune ha portato all'inserimento nei programmi della Scuola di *Corsi Vittorio Occorsio*, destinati ai funzionari e agli ufficiali di alto livello, provenienti anche da altri Paesi, che partecipano ogni anno alla formazione strutturata che la Scuola offre. I corsi esplorano, con modalità anche laboratoriali e con l'apporto di esperienze di diversa origine, gli strumenti di indagine e processuali, necessari per affrontare le nuove tecnologie.

Analoghi corsi vengono ogni anno organizzati presso la Scuola Superiore della Magistratura.

Il Seminario si inserisce in questo percorso e siamo quindi davvero lieti e onorati di poterne pubblicare gli atti nel Quaderno della Rivista Trimestrale della Scuola di Perfezionamento per le Forze di Polizia, che già ha visto altri contributi della Fondazione. La pubblicazione è anche in lingua inglese, per consentirne il pieno utilizzo da parte di tutti i frequentatori della Scuola. Essa potrà costituire la base per ulteriori riflessioni e per il lavoro di collegamento tra Accademia, Forze di Polizia e Magistratura che è obbiettivo primario della Fondazione.

Il seminario è focalizzato su come rendere effettivo l'esercizio della giurisdizione per i crimini transnazionali più gravi, commessi in tutto o in parte nello Spazio Virtuale, e su come rapportare la giurisdizione all'esercizio di altri poteri sovrani che a loro volta stanno affrontando processi di trasformazione rispetto alle sfidanti transizioni tecnologiche.

La transnazionalità è intrinseca al cybercrime. I cybercrimes più gravi possono riguardare anche infrastrutture critiche di una Nazione. Negli ultimi anni, le maggiori infrastrutture di alcuni Paesi sono state oggetto di attacchi di varia natura e di diversa gravità. Gli attacchi hanno riguardato anche i processi decisionali più sensibili in un regime democratico, quelli della formazione del consenso nelle elezioni, e quelli a supporto delle decisioni degli organi pubblici.

Le crescenti capacità di evolversi autonomamente da parte degli strumenti offensivi che si basano sull'IA di Frontiera rendono questi attacchi sempre più efficaci e le contromisure sempre più difficili.

Il G7 a guida giapponese ha prodotto, nell'anno passato, due importanti risultati circa la *Frontier AI* e circa la necessità di un approccio globale a queste sfide (*Hiroshima Process on AI*). IL G7 a guida italiana ha inteso proseguire su questa strada.

Senza la comprensione di queste dinamiche è vano affrontare i temi della difesa dagli attacchi cibernetici e delle sue implicazioni circa il dislocarsi dei poteri e delle garanzie.

Per questa ragione il seminario si apre con una rassegna delle più recenti e significative acquisizioni, da parte di ricercatori che hanno partecipato alla redazione di quelle conclusioni.

Le operazioni malevole condotte con strumenti informatici avanzati in realtà rilevano contemporaneamente per diversi aspetti che attengono alla sovranità nazionale. Un attacco informatico rivolto alle strutture critiche costituisce innanzitutto un delitto, secondo le previsioni della maggior parte dei Paesi. La Convenzione sul Cybercrime delle Nazioni Unite, in corso di approvazione da parte dell'Assemblea generale delle Nazioni Unite, prevede la necessaria punibilità delle condotte più gravi e si propone di universalizzare i

principi della Convenzione di Budapest, peraltro già sottoscritta da 75 Paesi.

Tali operazioni richiedono al tempo stesso una reazione dello Stato attaccato, volta a ridurre il danno e a prevenire danni futuri.

Gli attacchi, infine, costituiscono una violazione della sovranità e – nei casi più gravi – legittimano forme di reazione che possono giungere fino alla risposta cinetica contro lo Stato cui l'azione è attribuita.

I tre livelli di rilevanza dell'operazione malevola interferiscono tra di loro e richiedono quindi un serio coordinamento, innanzitutto a livello nazionale.

Interventi normativi recenti in Italia hanno innanzitutto esteso i poteri di azione volti alla resilienza (attribuiti all'ANC) e alla prevenzione attiva, nonché alla risposta offensiva, attribuita alle Agenzie di Intelligence; è stata inoltre rafforzata la possibilità di ricorrere a operazioni di infiltrazione, sotto copertura, volte all'acquisizione degli elementi utili per l'accertamento delle responsabilità ma anche all'interruzione della condotta in atto e alla *disruption* dello strumento informatico ostile.

Tra i problemi che tali novità pongono vi è il rapporto tra i tre livelli della reazione, perché essi non interferiscano tra loro, finendo per ostacolarsi a vicenda.

Centrale, dal punto di vista della giurisdizione, è ora il ruolo svolto dalla Procura Nazionale Antimafia e Terrorismo, organo cui è attribuito il ruolo di coordinare tali rapporti, mentre all'autorità giudiziaria e all'ANC fatto onere di operare salvaguardando le necessità diverse, dei due distinti e a volte contrastanti approcci. Basti pensare al tema della integrità della prova a fini penali, messa in forse dagli interventi difensivi immediati, in sé manipolativi.

Le potenziali interferenze sono molto ampie. Una in particolare merita specifica attenzione: l'efficacia di forme di cooperazione di intelligence, di polizia e giudiziarie ex post.

La giurisdizione deve affrontare la difficoltà derivante dalla transnazionalità delle operazioni, ulteriormente caratterizzate – nello specifico di cui trattiamo – da volatilità, opacità, non localizzazione, logica non deterministica e quindi difficile ricostruibilità a posteriori del percorso degli algoritmi. Tutto ciò implica che i meccanismi di collaborazione internazionale basati sul consenso successivo degli Stati all'acquisizione della prova sono di fatto inefficaci, almeno in alcune delle modalità di attacco.

Le difficoltà nella raccolta della prova sono comuni ai diversi sistemi ordinamentali. Gli Stati Uniti già da molti anni hanno predisposto uno strumento normativo per superare alcune di queste difficoltà, il *Cloud Act*. Esso tenta di superare il difficile ostacolo costituito dalla reale dislocazione dei poteri nello SV, tra Stati nazionali, Istituzioni sovranazionali e grandi gruppi privati.

Nonostante i significativi risultati ottenuti, anche gli USA hanno riconosciuto la difficoltà di esercitare efficacemente la giurisdizione penale nello SV. Recentemente, la *Deputy Attorney General* con delega per tale settore, Lisa Monaco, ha con chiarezza affermato che "*rather than focusing on arrests, US Law Enforcemen is trying to prevent additional victims of the crimes*" (24 aprile 2023). La conseguenza è che "*to combat cybercrime, US LE increasingly prioritises disruption*".

La duttilità dell'ordinamento statunitense consente questa prospettica limitazione, anche se qualcuno ha commentato che in passato ciò sarebbe stato considerato un'eresia ("*In days gone by, that might been heresy*"). Non vi è dubbio però che essa finisce per assimilare il processo penale, per sua natura volto all'accertamento di responsabilità personali per fatti previsti dalla legge come reato, alle altre forme di legittimo esercizio di poteri sovrani.

Nel nostro ordinamento, peraltro, una tale limitazione programmatica non sarebbe accettabile.

Gli Stati nazionali devono fronteggiare un non diverso problema, per le caratteristiche specifiche in cui esso si atteggia nello SV.

L'esercizio legittimo di poteri di reazione, ivi compresi quelli che si limitano alla violazione della sovranità di altre nazioni, a tacere di risposte offensive informatiche o cinetiche, deve infatti fare i conti con l'istituto della *attribuzione*, cioè con il raggiungimento della condivisione da parte della Comunità internazionale della provenienza dell'operazione malevola da uno o più Stati; come diretti attaccanti o come non adempienti agli obblighi di due diligence.

La sfida non è una *actio finium regundorum* tra diversi poteri dello Stato, per finalità di supremazia. La salvaguardia dell'effettività della giurisdizione nello SV è invece una assoluta necessità al fine di assicurare la trasparenza delle operazioni – fin dove è possibile e salvi i poteri concorrenti e legittimi di altri poteri dello Stato – e il rispetto della *Rule of Law*.

Anche gli organi della Intelligence sono, nel nostro ordinamento, soggetti al rispetto della legge e costituiscono parte dello Stato di diritto. Proprio queste caratteristiche, però, consentono l'azione coperta, tutelata dal segreto.

Dunque, la giurisdizione è anche una misura di protezione della Comunità internazionale contro il rischio di escalation, inestricabilmente connesso all'impiego di strumenti di penetrazione e reazione occulti. Ciò è tanto più rilevante se si considera l'intreccio tra le operazioni malevole e i conflitti, combattuti o striscianti.

Le potenzialità della futura guerra ibrida sono enormi, in parte ancora inesplorate. Ciò che ieri sembrava ancora lontano da venire è oggi realtà. I conflitti, in particolare quello ucraino, dimostrano le potenzialità offensive,

ancora in parte trattenute dalla consapevolezza dei rischi globali che possono discendere dall'impiego di ICT in forme occulte. L'impiego di armi autonome letali (*Autonomous Lethal Weapons* – ALW), di droni in grado di operare in massa, di realtà aumentata in grado di valutare la situazione sul campo, si è affermato come ordinaria realtà dei nuovi conflitti.

Le implicazioni sono enormi e non ancora del tutto analizzate. Il vantaggio competitivo delle ALW è tanto più alto quanto meno funzionano i meccanismi di autorizzazione da parte dell'essere umano. Il paradigma dello *Human in the Loop*, o addirittura in *Command*, rischia di rimanere una prescrizione etica, ben presto annebbiata dalla necessità che lo strumento sia in grado di competere con altri analoghi, ma non sottoposti a vincoli da parte di Nazioni che non intendono sottomettersi a quel precetto. In termini normativi, non solo etici, queste prescrizioni si affermano come obblighi di inserimento *by default* di meccanismi limitativi (autorizzazione, consenso, controllo ecc.), come previsto in generale dall'*EU IA Act* (in assenza di una regolamentazione sovranazionale delle ALW). Ma non tutti gli Stati aderiscono a questa impostazione e acquisiscono così un vantaggio competitivo enorme, rispetto ad apparati più lenti e meno precisi perché necessitanti del controllo umano.

Ma non è tutto. L'applicazione – di cui nulla sappiamo per ovvie ragioni di segretezza – di logiche sempre più avanzate e complesse, può determinare il rendersi autonomo dell'apparato munito di IA di Frontiera, quale definita ad esempio nell'UK *Frontier IA*, di cui si è detto e che costituisce oggetto di analisi nel seminario.

La sfida è dunque molto complessa. Essa finisce per incidere sugli stessi meccanismi di cooperazione internazionale, rendendo obsoleti quelli basati sul consenso successivo – destinati ad essere del tutto inefficaci nelle operazioni transnazionali cyber – e dovendo di conseguenza puntare su strumenti di cooperazione strutturati in anticipo e dunque basati sul consenso preventivo degli Stati alla interferenza nella loro sfera di sovranità. E' la direzione verso cui vanno sia la Convenzione di Budapest e il su Secondo Protocollo Addizionale, sia lo schema di Convenzione delle Nazioni Unite sul Cybercrime.

Ma queste misure non consentono di operare efficacemente nei confronti azioni malevole, in particolare di quelle costituenti reato, da parte di soggetti e di Stati che non si sottopongono alle previsioni delle Convenzioni, alle quali peraltro al momento aderiscono una minorità degli Stati.

Emerge quindi il grave problema di diritto interno e di diritto internazionale su quali azioni siano legittime per reagire a tal genere di attacchi. Innanzitutto, ponendosi di conseguenza il tema della attribuzione, ai fini del

riconoscimento da parte dalla Comunità internazionale della legittimità delle reazioni da parte dello Stato attaccato. In secondo luogo, delle modalità e dei limiti (di legittimità e di efficacia) dello strumento del diritto penale, un tempo epitome della sovranità nazionale.

Queste tematiche possono essere sintetizzate in quattro aree, che sono oggetto del seminario, che li ha visti sviluppati anche nel serrato dibattito tra i relatori e il pubblico:

a) Limiti della cooperazione internazionale multilivello, derivanti dalle caratteristiche specifiche dello SV
b) Strumenti per rendere effettiva tale cooperazione (stabilizzazione dei Corpi di investigazione comune e previsione della convalida successiva)
c) Azioni che gli Stati nazionali possono compiere legittimamente, secondo il diritto pubblico internazionale, per difendersi da attacchi provenienti da Paesi non cooperanti; condizioni e limiti
d) Strumenti giuridici attualmente a disposizioni in Italia (Intelligence e *Law Enforcement*) per agire nei casi sub c)

Infine, lo stesso dibattito pubblico su questi temi può essere compromesso dalle azioni malevole nel cyberspace. I meccanismi di disinformazione influiscono sulla fiducia nello spazio pubblico, minando una delle componenti essenziali della democrazia. Diventa profetica la battuta dei Fratelli Marx: "insomma a chi credi, a me o ai tuoi stessi occhi!?".

La giurisdizione non è la soluzione ma solo una parte di questa. Una parte forse minore ma di notevole rilevanza. Obiettivo del seminario, reso evidente dal dipanarsi degli interventi nelle quattro sessioni, è quello di individuare quali siano gli spazi per la effettività – e non solo la prescrizione – della giurisdizione, in rapporto all'esercizio di altri poteri, manifestazione legittima e sempre più invadente della sovranità.

SESSIONE INAUGURALE

PRESENTAZIONE DELLA FVO E MEMORIA DI VITTORIO OCCORSIO

Vittorio Occorsio
Co-fondatore FVO

A nome della Fondazione Vittorio Occorsio e di mio padre Eugenio, vi do il benvenuto a questo importante convegno dedicato a due temi di straordinaria attualità e rilevanza: la giurisdizione nello spazio virtuale e il ruolo dell'Intelligenza Artificiale nelle dinamiche giuridiche.

L'era digitale ha trasformato radicalmente il nostro modo di vivere, di interagire e di fare affari. In particolare, internet e le tecnologie più avanzate hanno abbattuto confini fisici e geografici, aprendo scenari giuridici del tutto inediti e complessi.

La nozione stessa di spazio, che sarà oggetto del convegno, ha subito un cambiamento epocale. Oggi il concetto di spazio fisico coesiste con quello di spazio virtuale, un ambiente in cui individui, aziende e governi operano attraverso reti digitali, spesso senza considerare la territorialità. Tuttavia, questa trasformazione pone sfide cruciali al diritto, che tradizionalmente si fonda su confini nazionali e su norme giurisdizionali ancorate alla fisicità degli Stati. In questo contesto, uno dei principali interrogativi è come possiamo definire e regolamentare la giurisdizione in uno spazio che non ha confini tangibili.

Ecco, potrei proseguire con questo tenore, se non che, quando stavo preparando il discorso nei giorni precedenti, ho fatto un esperimento e ho chiesto a Chat GPT di generare una relazione introduttiva a un convegno sullo spazio virtuale. Chat GPT mi ha generato i due capoversi che vi ho appena letto. Mi è apparso evidente di dover cambiare approccio.

Il mestiere degli introduttori dei convegni è, in effetti, uno dei più prossimi alla sparizione.

Visto che gli interventi tecnici saranno tanti e più qualificati del mio, preferisco allora parlare di qualcosa che Chat GPT non può replicare: i sentimenti. E sono due i sentimenti con i quali partecipo a questa introduzione dei lavori. Il primo, devo dire, è un sentimento di tristezza e di vuoto. Non sarei ovviamente qui se mio nonno, magistrato, non fosse stato ucciso nel 1976 qui a Roma da un gruppo terrorista di matrice fascista, vittima, come tanti altri,

negli anni di piombo, in quella stagione che dal 1969 al 1984 ha insanguinato il Paese. Vittima innocente, ma consapevole. Occorsio aveva colto una serie di correlazioni tra la malavita organizzata, anche di stampo mafioso, e poi la malavita romana che avrebbe generato la Banda della Magliana, alcune organizzazioni eversive di estrema destra, e infine alcune organizzazioni occulte internazionali e nazionali. Pochi giorni prima di essere ucciso aveva avviato un filone di indagine sui rapporti tra i sequestri di persona, la malavita organizzata e una Loggia massonica, che si sarebbe poi rivelata essere la Loggia Propaganda 2, di Licio Gelli. Cinque anni prima del sequestro di Castiglion Fibocchi.

La sua vicenda professionale e umana è stata forse unica, perché, pubblico ministero nel processo di Piazza Fontana e avendo arrestato Valpreda, fu accusato dagli anarchici e dalla sinistra di essere un conservatore. Poi, quando fece dichiarare illecita – per ricostruzione del partito fascista – il movimento "Ordine Nuovo", i neofascisti dissero che era dall'altra parte. Sballottato da una parte all'altra, alla fine ha pagato un prezzo altissimo.

Il secondo sentimento è opposto al primo, è un sentimento di gioia e di orgoglio: l'emozione di vedere il frutto del lavoro della nostra Fondazione. Quando l'abbiamo costituita nel 2020, e se lo ricordano Giovanni Salvi e Stefano Lucchini – cui va la mia profonda gratitudine – volevamo creare uno spazio di libertà, dove si incontrassero le migliori energie del paese, per custodire la memoria del nostro passato e, al tempo stesso, ragionare sul nostro futuro. Non intendiamo essere custodi delle ceneri, ma pensiamo che, per mettere a fuoco il futuro, la consapevolezza di chi e del come ci ha consentito di vivere in questo Paese, con questi valori, sia imprescindibile. Non possiamo dare nulla per scontato, come dimostrano le guerre, le discriminazioni, le violenze, il nuovo imperialismo tecnocratico, cui assistiamo.

Uno spazio di libertà, perché tutte le persone che generosamente prestano il proprio tempo per la Fondazione sanno che non vi sono strutture ideologiche precostituite e che il confronto e il rispetto delle idee degli altri è l'essenza dei nostri valori. Libertà, ovviamente, non è anarchia, e anzi, consapevolezza di valori etici profondi, non sbandierati in modo a volte banalizzante. Rispetto per l'altro, che è il contraltare della libertà, rispetto delle persone che lavorano, e qui ce ne sono state molte per questo convegno. Innanzitutto desidero ringraziare la Professoressa Melina Decaro, Segretaria generale della Fondazione e a cui si deve non solo l'impegno del coordinamento organizzativo ma il contributo di riflessione sulle implicazioni costituzionali dei temi che oggi affrontiamo. Ringrazio poi: Tiziana, Jasmin, Carola, Andrea, Joseph, Filippo, tutte le persone della nostra Fondazione che hanno lavorato, gli altri enti che hanno collaborato. Penso ad esempio a Coldiretti,

all'osservatorio Agromafie, alla professoressa Eugenia Carfora, preside del Liceo di Caivano. Qui avete visto in divisa e vi hanno accolto i ragazzi dell'Istituto Morano, con cui la nostra Fondazione lavora da tempo, siamo felici di averli oggi, anche in questo diverso contesto.

In tutti coloro che generosamente partecipano alla vita della Fondazione ho visto ideali profondi e valori, da cui deriva soddisfazione e speranza, nel memore ricordo di una stagione dove quegli ideali e valori hanno portato alla morte violenta di molti. Ieri, ad esempio, è stato l'anniversario di Girolamo Tartaglione, altro magistrato ucciso a Roma due anni dopo Vittorio Occorsio, questa volta dalle Brigate Rosse.

I volti delle vittime degli anni di piombo, del terrorismo, di tanti Magistrati, Carabinieri, Guardia di Finanza, Polizia, che hanno lottato per darci il modo di vivere libero che oggi conosciamo, li rivediamo nei loro colleghi, nei loro allievi. È una gioia vedere che la Fondazione è casa per i magistrati e le Forze dell'ordine, impegnati nel lavorare per il futuro, avendo sempre la memoria verso il passato.

Al convegno che si apre si parlerà della difesa della Repubblica, della difesa degli Stati nazione. Ecco, la difesa si sposta su altri piani, quello della tecnologia avanzata, ma richiede sempre - sottraggo un'espressione cara a Giovanni Salvi – *l'antica virtù del coraggio*, dai tempi della difesa della Repubblica di Atene a oggi, allo spazio virtuale: oggi come ieri, è al coraggio di noi tutti che dobbiamo far riferimento. Buon lavoro.

PRESENTAZIONE DEL SEMINARIO

Stefano Lucchini
Vice Presidente Comitato scientifico FVO - Chief Institutional Affairs and External Communication Officer di Intesa Sanpaolo

Buongiorno a tutti e benvenuti, sono Stefano Lucchini.

Grazie, Vittorio. Io non posso che essere contento e ringraziare intanto tutti i partecipanti e aggiungere una cosa personale. La passione che riesce a coinvolgere la Fondazione non posso che attribuirla e esserne grato sia a Giovanni Salvi, che è stato l'animatore, sia a Vittorio e a Eugenio Occorsio.

Mi associo ai ringraziamenti alla professoressa Carfora e agli amici della Coldiretti. Ringrazio il Ministero degli Esteri per questa ospitalità e la squadra, per l'organizzazione.

Vorrei provare ad articolare questo mio breve intervento introduttivo in tre parti.

Nella prima parte mi piacerebbe ragionare sulle trasformazioni tecnologiche, sociali ed etico-costituzionali in atto, partendo dal tema che oggi ci riunisce in questa splendida cornice.

Vorrei, in particolare, partire dalle prime due parole con cui esordisce il titolo che si è voluto dare a questa importantissima occasione di studio e di riflessione: "spazio virtuale". Lo interpreto come un quasi provocatorio richiamo a quello che, in passato – perché è sempre importante cogliere insegnamenti dal passato – è stato considerato la caratteristica principale del cyberspazio: uno spazio, quello del mondo dei bit, per l'appunto, di natura virtuale, quasi in opposizione allo spazio reale proprio del mondo degli atomi.

Facciamo un passo indietro di qualche anno, in modo da cogliere in pieno quelle lezioni del passato a cui facevo riferimento, ed evitare, oggi che ci si accinge a regolare l'asse complesso dell'ecosistema digitale costituito dall'Intelligenza Artificiale, di compiere gli stessi errori o, semplicemente, ingenuità.

Questi errori hanno caratterizzato il dibattito originario sulla regolazione del web. Davos, 1997, World Economic Forum: *Governi del mondo, stanchi giganti di carne e acciaio, io vengo dal cyberspazio, nuova dimora della mente. A nome del futuro, chiedo a voi, esseri del passato, di lasciarci soli. Non siete graditi fra di noi. Non avete alcuna sovranità sui luoghi dove ci incontriamo*.

Naturalmente, sono provocazioni. Se ci fosse ancora qualche dubbio su come venisse concepito l'ordinamento della rete dai padri fondatori del perio-

do iniziale del web, questo passaggio della *Dichiarazione di indipendenza del cyberspazio* di Barlow potrebbe essere utile per dissiparli. Si tratta di un ordinamento, o meglio di un nuovo immaginato ordine virtuale, caratterizzato da una discontinuità assoluta rispetto all'ordinamento statale, non solo per il distacco e la separazione spazio-temporale da quest'ultimo, ma anche per la valenza rivoluzionaria attribuita alla comunità della rete, in grado di autoregolarsi senza alcun filtro delle istituzioni, dei poteri pubblici e delle formazioni sociali di carattere intermedio, caratterizzati da quell'*humus* strutturale dell'ordinamento giuridico inteso in senso romano.

Quasi trent'anni dopo, è facile concludere come la storia abbia fatto emergere una realtà assai diversa da quella che si augurava Barlow. Forse meglio, per almeno due ragioni.

La prima è che gli Stati-nazione hanno dimostrato di poter non solo regolamentare, ma anche iper-regolare il cyberspazio, che è bene sempre tenerlo a mente: prima ancora che di bit, è costituito da infrastrutture fisiche, cavi sottomarini e quindi da una dimensione atomica, parte di quel mondo analogico nei cui confronti Barlow si autoproclamava ribelle. Gli stati, oggi, si sono mostrati in grado di creare grandi muraglie virtuali, come nel caso del Great Firewall cinese e, ultimamente, quello russo, a seguito dell'invasione dell'Ucraina, che vede muraglie virtuali e strategie che doveva essere, secondo la visione utopistica dei pionieri della nuova frontiera digitale, un nuovo mondo libero da condizionamenti e poteri forti, in cui la continuità di utenti avrebbe avuto la capacità di autoregolarsi alla luce di una cornice valoriale di riferimento fondata sulla libertà della rete e nella rete, si è rivelato uno spazio che, lungi dal voler cavalcare le visioni altrettanto nocive di quelle utopistiche e distopiche, per esempio di Morozov e parzialmente anche di altri personaggi, si è rivelato assai accessibile ai poteri privati che hanno sicuramente condizionato quel processo di autodeterminazione da parte degli utenti, che doveva essere la pietra angolare su cui costruire lo spazio immaginato dai pionieri del web.

È questo, a mio avviso, l›humus concettuale all›interno del quale possono essere inquadrate le prospettive assai stimolanti e complementari che caratterizzano queste due giornate di lavoro. Siamo molto curiosi di capire e vedere cosa emergerà poi in una sintesi da queste due giornate così importanti. La seconda parte di questo intervento vuole invece concentrarsi sull'identificazione di qualche interrogativo di fondo che mi sembra poter caratterizzare un comune denominatore, un filo rosso, di questi temi che saranno autorevolmente sviluppati in queste due giornate. Si dice spesso che la vera difficoltà nel costruire un percorso di indagine innovativo non risiede nel darsi le giuste risposte, ma nel formulare le domande più adeguate ad aprire tale percorso.

E così ci siamo fatti qualche domanda, senza ambizioni di esclusività. Potrebbe forse essere utile per i lavori di queste due giornate indagare quali sono le ragioni della trasfigurazione in corso delle grandi piattaforme tecnologiche da semplici attori economici a veri e propri poteri privati, spesso in competizione con quelli pubblici. È proporzionale e adeguata la trasformazione dello strumento regolamentare europeo per far fronte a tale trasfigurazione? E ancora, quali sono le nuove sfide che pone l'emersione dell'Intelligenza Artificiale di tipo generativo? Perché essa richiede una reazione regolamentare, ma anche una cornice costituzionale di contenimento differente rispetto a quelle che hanno caratterizzato la reazione all'emersione del fattore algoritmo? E quale, infine, la differenza in termini di principi costituzionali in gioco tra automazione alla base della stagione dell'algoritmo e autonomia, accelerazione spazio-temporale, inferenza e predittività, che integrate costituiscono invece le caratteristiche essenziali del nuovo ecosistema digitale costituito da questa Intelligenza Artificiale che è così prorompente in questi ultimi anni?

Lascio a voi provare a dare delle prime risposte a questi interrogativi, ammesso che li consideriate interessanti, naturalmente. E infine, l'ultima parte di questa breve introduzione, alla luce delle riflessioni che ho provato a sviluppare in apertura. E' chiaro che le questioni oggetto di indagine e riflessioni oggi sono tutt'altro che virtuali. Sicurezza nazionale, sovranità, territorio sono categorie del diritto costituzionale che sono ancora, come l'attualità ci conferma, vive e vegete anche nel cyberspazio e hanno un impatto reale, tangibile sulla vita quotidiana di tutti noi.

Lasciatemi concentrare sulla questione della protezione della sicurezza nazionale, oggetto privilegiato.

Come notato recentemente in un bell'articolo del Sole 24 Ore del Prefetto Frattasi e del Professor Pollicino, nel volgere degli ultimi anni la cybersicurezza e le questioni ad essa connesse, trattate in modo sempre più sistemico, fanno emergere preoccupazioni per la tenuta, tra le altre cose, anche dello Stato di diritto. Si sono poste progressivamente al centro dell'attenzione generale, andando ben oltre la dimensione di nicchia per specialisti che ha caratterizzato i primi passi, sia dal punto di vista dell'interesse della dottrina, specialmente per quanto riguarda le implicazioni istituzionali, sia della giurisprudenza.

In tal contesto, la cybersicurezza si sta ponendo sempre più come un diritto fondamentale della persona, dotato di una sua autonomia assiologica e concettuale. Non vi è ancora un riconoscimento del diritto alla cybersicurezza inteso come autonoma posizione sostanziale della persona. Tuttavia, un cambiamento di approccio è già presente anche in ambito nazionale, in conside-

razione dell'ampliamento del numero dei soggetti destinatari della disciplina rilevante in materia di cybersicurezza, la cui piena attuazione ridonda nella tutela del cittadino dalla minaccia alla sua libertà nella dimensione digitale, dando seguito anche in quest'ultima dimensione a una concezione prismatica della sicurezza, da tempo evidenziata nel dibattito pubblico.

Mi avvio alla conclusione. A mio avviso, una bussola per i lavori di oggi e più in generale per le grandi sfide di questa accelerazione al cambiamento, potrebbe essere proprio guardare alla sicurezza quale diritto di libertà, come d'altronde costituzionalmente sancito dall'articolo 5 della Carta dei Diritti Fondamentali dell'Unione Europea, laddove prevede espressamente che ogni individuo ha diritto alla libertà e alla sicurezza. Codifica quel binomio concettuale libertà e sicurezza che sarebbe assai pericoloso scindere. Grazie.

SALUTI ISTITUZIONALI

Riccardo Guariglia

Segretario generale del Ministero degli Affari Esteri e della Cooperazione Internazionale

Sono Riccardo Guariglia, Segretario generale del Ministero degli Esteri, e anche a nome del Ministro Taiani desidero dare il benvenuto alla Farnesina. Come sapete, la Farnesina è la casa della diplomazia italiana, una casa dalle porte sempre aperte, soprattutto per le iniziative internazionali che attengono agli interessi vitali del nostro paese. A questo proposito, devo dire che la collaborazione con la Fondazione Occorsio è per noi motivo di prestigio, e dunque vi ringrazio per aver scelto come sede per questo importantissimo seminario proprio la Farnesina, sulla quale potete sempre contare. L'evento di oggi costituisce un'iniziativa che tenevamo molto ad ospitare, proprio in ragione dell'alto valore scientifico e della centralità dei temi prescelti. Mi complimento con la Fondazione per l'altissimo livello dei relatori e degli ospiti, primo fra tutti, naturalmente, il ministro che ci onora della sua presenza qui, così come per la ricchezza del programma che è stato delineato per la giornata di oggi. Nel contesto delle crisi che attraversano lo scenario internazionale odierno, sarebbe un errore trascurare fattori quali il quinto dominio, cioè lo spazio cibernetico, nonché la trasformazione digitale. Infatti, nel cyberspazio, le dinamiche geopolitiche assumono oggi una dimensione, per così dire, più sfuggente rispetto agli strumenti di quella che noi consideriamo la cassetta degli attrezzi dei diplomatici e di tutti gli addetti ai lavori. Si tratta di un dominio popolato da molteplici attori, non sempre benevoli: penso ai gruppi che conducono campagne di disinformazione e che attaccano infrastrutture critiche, o ancora ai soggetti che perpetrano varie attività criminali, e mi riferisco non soltanto a persone fisiche e società, ma anche a entità statuali.

Quindi è un rischio veramente importante. D'altra parte, il progresso tecnologico ha messo a disposizione di tutti gli utenti strumenti sempre più all'avanguardia e sofisticati, che richiedono sia ingenti investimenti sia regole efficaci. Proprio le nuove tecnologie portano tali problematiche a un livello ancora più complesso. Siamo tutti affascinati dalle strabilianti potenzialità dell'Intelligenza Artificiale, e la fantasia corre lungo le trame di libri e romanzi – già ce ne stanno che trattano proprio di questo argomento – e varie applicazioni di tale tecnologia possono davvero migliorare le nostre vite in campo sanitario, nella prevenzione delle crisi e dei disastri, nell'erogazione di servi-

zi pubblici e privati, nell'erogazione di servizi finanziari, ma ci sono molti altri campi che vengono toccati. Quanto realmente sappiamo dei rischi che ne possono derivare? Questo impatto sul mondo del lavoro, sulle categorie più vulnerabili, sulle stesse relazioni internazionali, quali risvolti giuridici determina? Il nostro Ministero annette particolare rilievo al tema della sicurezza cibernetica e alle nuove tecnologie, tanto che abbiamo voluto creare, sotto l'impulso del ministro Tajani, un'apposita unità presso la segreteria generale che io dirigo. Siamo impegnati per promuovere un cyberspazio aperto, libero, ovviamente interoperabile e sicuro in ambito G7. Il nostro impegno risale alla presidenza italiana del 2017: ricordo quando, proprio in quell'occasione, fu adottata la dichiarazione di Lucca dei ministri degli Esteri. Ero presente e ricordo il primo documento politico del G7 sulla sicurezza cibernetica, un vero riferimento per le presidenze successive. In coerenza con questo precedente, quest'anno la Farnesina ha presieduto il gruppo di lavoro Ise-Shima (Ise-Shima Cyber Group – ISCG), che ha trattato aspetti di cyberdiplomazia, mentre l'Agenzia per la cybersicurezza nazionale ha convenuto, a maggio, proprio in questa sala, per la prima volta, le omologhe agenzie dei paesi G7 e dell'Unione Europea.

Ho tenuto a inaugurare tutti e due questi eventi per il rilievo proprio della tematica nel contesto della nostra politica estera. Grande importanza è stata poi annessa ai dossier dai Ministri degli Esteri, della Giustizia, dell'Interno, nonché di Stato e di Governo riuniti a Borgo Egnazia sotto l'egida del G7 a presidenza italiana. In un mondo costantemente connesso, il cyberspazio è sempre più conteso ed è divenuto veicolo di campagne malevole, spesso collegate a obiettivi di politica estera. Ed è proprio per questo che i paesi del G7 hanno espresso preoccupazione per il crescente numero di attacchi cyber, soprattutto ransomware, contro ospedali e strutture sanitarie. Abbiamo ribadito la ferma determinazione a proteggere i nostri sistemi democratici e le infrastrutture critiche, richiamando il comportamento responsabile degli Stati nel cyberspazio e l'applicabilità del diritto internazionale. Sono questi, del resto, gli stessi principi per i quali ci battiamo in tutti i consessi multilaterali: penso alle Nazioni Unite, all'Unione Europea, alla NATO, all'OSCE, al Consiglio d'Europa e nei contatti bilaterali che abbiamo con i paesi allineati e non. Lo scopo è l'attuazione di specifiche misure di costruzione della fiducia, fiducia che è necessaria anche quando guardiamo alle nuove tecnologie e prendiamo in considerazione l'Intelligenza Artificiale. Fiducia significa studiare insieme gli aspetti tecnico-scientifici dello strumento e, al tempo stesso, elaborare insieme un quadro normativo importantissimo in grado di fissare barriere etiche a tutela della centralità dell'essere umano. È questo lo spirito che anima e che ha animato fino adesso il nostro impegno durante la presidenza del G7, nella

cui agenda, come ho citato poc'anzi, il Presidente del Consiglio ha voluto attribuire all'Intelligenza Artificiale un carattere veramente prioritario. Lo scopo è elaborare politiche adeguate che consentano di cogliere appieno i vantaggi di tali tecnologie, mitigando i rischi per la società. Questo è il *fil rouge*, il *leitmotiv* del nostro lavoro.

A tale scopo si rivela essenziale la definizione di una governance internazionale dell'Intelligenza Artificiale, sfida considerevole, dati i diversi approcci e sensibilità a ogni latitudine del globo. E anche su questo fronte, l'Unione Europea ha dimostrato la propria capacità di porsi come punto di riferimento per l'intera comunità internazionale, avendo approvato, a maggio, come sapete, con il determinante contributo del nostro Paese – è importante sottolinearlo – il regolamento *Artificial Intelligence Act*, primo set di regole vincolanti sull'Intelligenza Artificiale. Signore e signori, e concludo, i temi ai quali ho poc'anzi accennato e che saranno al centro di questi due giorni di lavoro meritano indubbiamente qualificati approfondimenti giuridici, poiché dal cyberspazio e dalle nuove tecnologie molto dipende nello sviluppo delle relazioni internazionali e, più in generale, nel percorso di crescita dell'umanità. Il diritto è, sin dai suoi albori, tra l'altro in gran parte avvenuti a Roma, uno strumento duttile, capace di adattarsi alla mutevole realtà socioeconomica per offrire ad essa disciplina efficace. Ci vuole, naturalmente, un grande impegno, grande determinazione e, come ha detto Vittorio Occorsio, lo vorrei sottolineare, grande coraggio. Sono assolutamente d'accordo, è una simile sfida alla capacità di normalizzazione del diritto, che si ripete oggi con il quinto dominio, una sfida affascinante sulla quale sono certo si susseguiranno oggi e domani autorevolissimi interventi. Grazie a tutti quanti e buon lavoro a tutti.

Giuseppe Amato

Procuratore generale presso la Corte d'Appello - Responsabile per le autorizzazioni delle intercettazioni delle Agenzie di informazione per la sicurezza

Grazie per l'invito gradito, di cui sono veramente riconoscente. Non posso non partire, come ha fatto Vittorio, da due considerazioni sui temi di cui oggi dobbiamo parlare. Non posso non partire anche io da un ricordo, il ricordo di Vittorio Occorsio, che abbiamo commemorato il 10 luglio di quest'anno. Per me è un ricordo particolare, perché ha accompagnato la mia infanzia e tanti rapporti personali che avevamo con nonno Vittorio. Un ricordo doveroso e un vero apprezzamento per ciò che la Fondazione fa e farà per affrontare temi importanti come quello di oggi. Questo ricordo deve essere anche uno stimolo per guardare avanti. Proprio riallacciandomi a questa esigenza di trovare stimoli, il convegno di oggi è particolarmente significativo.

Vittorio Occorsio è una vittima del terrorismo, e oggi parliamo di cybersicurezza. Parlando di cybersicurezza, si affronta anche il contrasto agli attacchi che possono avere una finalità terroristica. Questo rende il tema di grande attualità. Considerando una nozione ampia di terrorismo, certi attacchi informatici rientrano pienamente in questa categoria, data la loro capacità di interferire in modo significativo con le strutture politiche, economiche e imprenditoriali di un paese. Quindi, la cybersicurezza è anche una lotta al terrorismo.

Le procure italiane, da anni, nel contrasto alla criminalità informatica, sono organizzate valorizzando la specializzazione dei magistrati. In alcune procure, il contrasto ai reati informatici è attribuito a coloro che fanno parte dei gruppi di contrasto al terrorismo. Ricordo il periodo dal 1993, con la prima legge organica italiana sui reati informatici, alla Convenzione di Budapest, fino alla legge che l'ha attuata. In quegli anni eravamo pionieri nel contrasto ai reati informatici. Ho avuto l'opportunità, con alcuni colleghi, di scrivere un libro sul tema nei primi anni 2000. Rivedendolo oggi, si nota come molti argomenti allora fondamentali siano ormai superati. All'epoca si discuteva persino sulla definizione di documento informatico e di sistema informatico, mentre oggi parliamo di spazi virtuali ancora da riempire di contenuto, in un'epoca di cambiamento.

Il nostro ordinamento ha compiuto progressi significativi da allora. Con l'istituzione dell'Autorità per la Sicurezza Cibernetica nel 2021, è stato compiuto un passo importante per il coordinamento tra i vari attori del contrasto alla cybersicurezza. Questo coordinamento non è fine a se stesso, ma deve essere proattivo, valorizzando le diverse risorse disponibili. Ulteriori passi avanti sono stati compiuti con il decreto legge del 2023, che ha previsto un

coordinamento per certi reati presso la Procura Nazionale Antimafia, evidenziando l'importanza di un approccio proattivo, soprattutto in un contesto in cui la territorialità è sempre più marginale. Successivamente, la legge del 2024 ha rafforzato sia gli strumenti a disposizione della magistratura sia quelli preventivi, responsabilizzando tutti i soggetti le cui reti possono essere oggetto di attacchi.

Abbiamo a disposizione uno strumentario importante che consente di affrontare il fenomeno in modo significativo. Vorrei fare due riflessioni basate sulla mia esperienza di magistrato e attualmente di Procuratore Generale a Roma, con particolare attenzione alle intercettazioni e ai servizi. La prima riflessione riguarda l'importanza del contributo della magistratura, non solo in un'ottica di repressione, ma anche di prevenzione. La prevenzione è fondamentale: la repressione è già una sconfitta, poiché implica che l'attacco sia stato già commesso. In questo ambito, è decisivo un approccio preventivo per evitare che i danni si concretizzino.

La seconda riflessione riguarda l'attività delle Agenzie e delle intercettazioni telematiche, che sono fondamentali per prevenire infiltrazioni, dossieraggio e abusi. Ritengo che il nostro sistema sia un esempio di garanzia, grazie alla presenza di un'autorità indipendente, al rispetto della normativa e al controllo delle autorità politiche. Questo sistema consente di unire prevenzione e repressione in modo efficace, garantendo sicurezza e rispetto delle libertà fondamentali.

Concludo esprimendo fiducia nella capacità del nostro sistema di contrastare efficacemente questi fenomeni e rimango in attesa di approfondire le prospettive future, anche in vista della nuova convenzione delle Nazioni Unite che potrebbe portare ulteriori cambiamenti normativi.

Fabio Pinelli
Vicepresidente Consiglio Superiore della Magistratura

Le nuove tecnologie e in particolare l'applicazione dell'intelligenza artificiale al settore giuridico portano con loro una serie di conseguenze pratiche – in larga parte ancora imprevedibili – e stimolano una riflessione, affascinante e spaventosa insieme, sulle sue ricadute in termini di tutela dei diritti fondamentali e di ruolo della giurisdizione.

Molto opportunamente questo Seminario – che pur nel titolo non menziona espressamente l'intelligenza artificiale – ha dedicato il suo focus ai due termini più problematici che la evocano: lo "spazio virtuale" e le "garanzie di giurisdizione".

Le nuove forme di criminalità consentite dalle nuove tecnologie (sulle quali si sono soffermate alcune relazioni) consentono di portare la pericolosità delle condotte attuate (ed attuabili) al livello della stessa sicurezza nazionale, ponendo quindi un problema di riorganizzazione della reazione ordinamentale, che è importante – per la salvaguardia stessa della democrazia e delle conquiste giuridiche e sociali che essa ha consentito – mantenere nei limiti di una risposta giurisdizionale, in cui inevitabilmente sembra giocare un ruolo centrale la giurisdizione penale: la tragica alternativa sarebbe infatti quella bellicista delle cd. cyber-guerre.

La risposta giurisdizionale si deve però adattare, per essere efocace, alle caratteristiche di tali "nuove condotte" e di tali "nuove forme di aggressione" a beni giuridici fondamentali, che la pongono di fronte a nuovi e in larga parte inediti limiti.

Il primo appunto è quello del cd. "spazio virtuale". In effetti, la capacità di azione – consentita da tecnologie digitalizzate, come quelle dell'intelligenza artificiale – non solo non è più limitata da confini territoriali, ma non presenta più neppure precisi punti di riferimento fisici: questo significa, infatti, il cd. cyber-spazio, che in realtà è un "non-spazio".

Tutto ciò rischia di mettere in crisi i tradizionali strumenti giuridici di determinazione della competenza per territorio e della stessa giurisdizione dei singoli Stati, facendo dei sistemi di intelligenza artificiale un obiettivo sfuggente e sostanzialmente non "catturabile" dai singoli ordinamenti.

Da qui l'esigenza – che pure è stata oggetto di alcuni interventi – che la sfida cooperativa tra i vari Stati non solo venga sentita come ineludibile, ma debba anche spingersi oltre agli strumenti tradizionali e sperimentarsi in nuove forme per contrastare questo "effetto despazializzante" dell'Intelligenza Artificiale e delle nuove tecnologie.

L'altro versante del problema della giurisdizione e della cooperazione–

insieme alle tradizionali garanzie che operano in esse – è quello dei meccanismi di imputazione della responsabilità (oggetto anch'essi di relazioni nel seminario).

Rispetto a nuove entità artificiali capaci di scelte autonome e capaci di azioni che un tempo erano possibili solo per un essere umano – inimmaginabili fino a pochi anni fa – si pone l'ulteriore e grave problema della responsabilità in sede giudiziaria delle "macchine".

Il dogma del machina delinquere non potest non regge più. Il modello tradizionale per il quale le macchine sono meri strumenti dell'agire criminoso umano non è più applicabile perché il risultato dannoso è causa della scelta della sola macchina, in modo sempre più scollegato dall'agire dell'uomo che l'ha costruita e che, per così dire, ha una "responsabilità genetica", che male si adatta ai tradizionali meccanismi imputativi del dolo e della colpa.

Esiste dunque il rischio evidente di un vuoto di tutela penale per taluni tipi di offesa, dal momento che i modelli imputativi di responsabilità oggettiva non sono compatibili con il principio di colpevolezza e personalità della responsabilità penale.

Gli stessi singoli agenti umani, "geneticamente" responsabili, sono occulti e difocilmente identificabili, posto che ciò che emerge è in larga parte il solo comparire delle condotte (sganciate da un agente umano e riferibili a Bot o simili) sulle varie "piattaforme".

Ecco, dunque, uno dei temi più delicati che si pongono in materia: in che termini si può parlare di "responsabilità delle piattaforme"? Quali rischi per la libera manifestazione del pensiero si possono annidare nell'attribuzione di queste forme di responsabilità? Quali resistenze globali vi si oppongono? Esse possono considerarsi superabili?

Di fronte a tutte queste difocoltà si potrebbe essere tentati dal dire che la migliore risposta non sia quella repressivo-sanzionatoria, ma quella preventiva, quella cioè di una normazione che si appunti sulla creazione, produzione e utilizzo di sistemi di intelligenza artificiale che agiscono in spazi virtuali.

Mi pare che questa sia, in fondo, la prospettiva del Regolamento europeo adottato il 13 giugno 2024, contenente regole armonizzate sull'intelligenza artificiale.

Lo scopo della normativa è certo quella di migliorare il funzionamento del mercato interno e promuovere la diffusione di un'intelligenza artificiale "antropocentrica e afodabile", garantendo nel contempo "un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione".

Tuttavia, prendere come specifico oggetto della normativa, la circolazione nei mercati dei sistemi di intelligenza artificiale, risponde all'idea che i sistemi di intelligenza artificiale sono un prodotto "rischioso", tanto che ne viene stabilita una classificazione, che comprende (in presenza di alcune caratteristiche) la qualificazione in termini di sistema ad "alto rischio", e viene prescritta una serie di garanzie e di requisiti per chi li produce, fornisce, diffonde e utilizza. Insomma – per essere più chiari, ma banalizzando un po' – i sistemi di intelligenza artificiale sono come "armi" e deve essere prevista una disciplina normativa che ne regoli la produzione, la diffusione e l'utilizzo: non può essere lasciata completamente alla libertà individuale e a meri meccanismi di mercato e, forse, neppure alle isolate decisioni di singoli Stati.

Infatti – ed è questa l'altra idea di grande interesse contenuta nella normativa europea – i limiti all'utilizzo di questi nuovi strumenti (nel rispetto della garanzia dei diritti fondamentali) si deve imporre anche agli Stati e nella stessa attività di repressione criminale da questi condotta: la scelta "garantista" non è un'opzione che si possa abbandonare a seconda delle emergenze e delle contingenze; deve considerarsi una scelta irrevocabile, connotante ogni sistema di democrazia liberale.

Una tecnologia così potente e pericolosa per i diritti della persona, come quella dei sistemi di intelligenza artificiale, non può essere valutata solo in termini di efocienza e di raggiungimento di risultati (seppure di repressione criminale), ma deve essere circondata da una serie di garanzie e di precauzioni peculiari e adeguate ai rischi che si corrono con il suo utilizzo.

Significativo, a mio avviso il fatto, che in attuazione di tali principi il regolamento si occupi, ad esempio, dell'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto, ponendo dei limiti precisi.

Quindi le esigenze della giustizia penale non consentono, nella prospettiva del regolamento, sempre e comunque l'utilizzo di sistemi di IA (nella specie sistemi di identificazione biometrica remota), ma richiedono "proporzione" (uso necessario), sono limitati solo a talune "esigenze" e solo per "reati gravi".

Questa mi pare una indicazione di metodo estremamente importante: il contenimento della nuova criminalità dello spazio virtuale attraverso la giurisdizione ha senso solo in quanto essa si mantenga nel rispetto delle garanzie dei diritti fondamentali che la costituiscono nei sistemi democratici.

Tuttavia, non sembra che esistano soluzioni ottimali e non ci si possono nascondere i limiti che questo tipo di interventi normativi comportano.

In primis, la sfasatura temporale che inevitabilmente si produce tra tempi per l'adozione e attuazione delle normative e sviluppo delle tecnologie, che continuano a fare passi avanti e ad accelerare sempre più.

In verità l'Italia si è attivata immediatamente e nel Consiglio dei ministri del 23 aprile scorso (circa un mese dopo la pubblicazione sulla Gazzetta Ufociale dell'UE del regolamento sull'IA) è stato approvato un disegno di legge in materia di intelligenza artificiale, che dovrebbe coprire cinque ambiti: strategia nazionale, autorità nazionali, azioni di promozione, tutela del diritto di autore e sanzioni penali; il disegno di legge di iniziativa governativa il 19 settembre 2024 era all'esame dell'VIII e IX Commissioni riunite; è poi già stato pubblicato il documento – redatto da un Comitato di esperti per supportare il Governo – contenente la strategia italiana per l'Intelligenza Artificiale 2024-2026.

Tuttavia, una certa dilazione temporale è necessitata dai tempi di attuazione, implicati non solo dalla necessità di adeguare le normative nazionali, ma anche per rispettare i diritti fondamentali previsti dall'UE a favore delle imprese produttrici e fornitrici e dare tempo anche ad esse di adeguarsi alle nuove norme. Queste ineliminabili necessità – collegate al sistema normativo e alle elevate garanzie che esso prevede – determina però un gap temporale che, in considerazione della rapidità di sviluppo di queste nuove tecnologie e delle loro applicazioni, rischia di presentare una normativa sempre in ritardo rispetto all'evoluzione di una tecnologia come l'intelligenza artificiale, tanto che da alcuni si è ipotizzato di utilizzare strumenti più utili e veloci come l'adozione di norme tecniche e standard che, però, essendo norme di cd. soft law, non hanno il grado di vincolatività della più lenta normazione di cd. hard law (cioè, regolamenti e direttive europee e leggi nazionali).

La mancanza allo stato di soluzioni ottimali rappresenta dunque una sfida che questo Seminario ha inteso affrontare con intelligenza – e con intelligenza umana – portandola al livello utile, che è quello di una collocazione significativa nell'ambito del G7.

Le nuove tecnologie e l'intelligenza artificiale rappresentano, infatti, una sfida ancora in corso per l'intelligenza umana, una sfida che però non è alla portata né dei singoli, né dei singoli Stati, ma una sfida che deve essere affrontata a livello globale e che è opportuno collocare a livello della giurisdizione, come sede di maggiore garanzia dei diritti fondamentali della persona, che rappresentano forse la maggiore conquista del moderno mondo giuridico.

Silvana Sciarra

Presidente della Scuola Superiore della Magistratura

Grazie, grazie davvero. Sono grata alla Fondazione Vittorio Occorsio per l'invito a porgere il saluto mio personale e della Scuola Superiore della Magistratura in un'occasione come quella di oggi, che è caratterizzata da un altissimo livello di oratori e di partecipanti e dalla rilevanza dei temi affrontati. Un saluto particolare al signor Ministro. La mia presenza conferma e vuole confermare una collaborazione ormai matura tra la Scuola Superiore della Magistratura e la Fondazione, una collaborazione feconda che speriamo continui sempre con toni ancora più accentuati su questi temi. Questo evento è, tra l'altro, un evento collaterale al G7 a presidenza italiana, che ha dato avvio tra l'altro ai lavori del *Venice Justice Group*, cui tutti guardiamo già nelle prossime settimane per cogliere un ulteriore impulso che si intende dare al contrasto al crimine organizzato in tutte le sue forme e declinazioni, nonché a un equilibrato ricorso all'Intelligenza Artificiale a tutela dei sistemi democratici. È stato ricordato e voglio ribadirlo, dello Stato di diritto, dunque della magistratura, da quel quadro di riferimento che io credo sia un quadro imprescindibile per una piena e consapevole trasposizione del regolamento europeo, anche questo appena ricordato, entrato in vigore lo scorso giugno, che stabilisce regole armonizzate in materia di Intelligenza Artificiale, ispirazione per l'attività della Scuola Superiore della Magistratura, sulla scorta, peraltro, di una programmazione di corsi da tempo avviata su questi e su altri temi connessi, per esempio sulla difesa della sicurezza nazionale e la riflessione sulla Convenzione di Budapest sulla Cyber Crime.

Non è superfluo ricordare che questo regolamento, che è stato opportunamente ricordato dall'ambasciatore Guariglia, si prefigge un migliore funzionamento del mercato interno nella libera circolazione di beni e servizi. Perché il mercato interno, bisogna ricordarlo agli europei, è in effetti un bene comune che, fin dalla Comunità del Carbone e dell'Acciaio, ha visto gli Stati fondatori tenuti insieme dalla fondazione di un mercato unico. E poi in questo mercato ci sono sempre inclusi altri Stati, quindi un mercato sempre più allargato. E questo mi piace ricordarlo perché la libera circolazione, è stato detto, è un esercizio di libertà, e anche la sicurezza è un esercizio di libertà. Ma ricordiamoci che ai tempi della Comunità del Carbone e dell'Acciaio veniva garantita la libertà di movimento dei minatori italiani che andavano spesso a lavorare con dedizione in Belgio e in Germania. Oggi le regole del mercato devono, invece, applicarsi all'Intelligenza Artificiale nel rispetto di principi trasparenti che non devono essere mai disgiunti dal rispetto di principi e diritti fondamentali e devono favorire la cooperazione giudiziaria. Il Consideran-

do numero uno del regolamento fa riferimento alla Carta dei Diritti Fondamentali dell'Unione Europea, un testo che non dobbiamo mai dimenticare, un testo che, tra l'altro, sul richiamo del Considerando numero uno, tutela la salute, la sicurezza come beni primari, ma anche lo Stato di diritto e l'ambiente. In questi processi di integrazione attraverso il diritto credo molto. I giuristi più anziani, fra i quali io mi colloco, devo dire fortunatamente, perché le età vanno vissute per quelle che sono, ricorderanno l'opera di un grande giurista italiano, Mauro Cappelletti, che studiava l'integrazione attraverso il diritto ed aveva superato i confini italiani. Ecco, io credo che in questa integrazione attraverso il diritto, in cui, ripeto, io credo molto, è cruciale il ruolo della formazione. Lo era già agli albori della Comunità Economica Europea, perché la formazione, appunto, è stato veicolo per l'esercizio pieno delle libertà garantite dai Trattati. E l'integrazione nell'Unione Europea è parallela e direi, forse funzionale, al miglior coordinamento delle misure statali nel contesto del Consiglio d'Europa. Quindi, l'integrazione dobbiamo interpretarla, e lo facciamo già da tempo, come un'integrazione a più livelli, specie per garantire la Cyber Security. La Scuola Superiore della Magistratura investe incessantemente, ci tengo a dirlo, con un'attività davvero capillare, energie e competenze nella formazione dei magistrati italiani e, nel contempo, contribuisce a orientare attività formative in altri Paesi. Non è soltanto l'impegno molto rispettato, devo dire, della Scuola nella rete europea delle scuole di formazione dei magistrati, ma anche l'opera di disseminazione di contenuti e tecniche formative che la Scuola Superiore della Magistratura svolge nei confronti di altri paesi. Sottolineo in particolare l'impegno con i paesi africani, cui avremo modo anche di parlare, vero l'ambasciatore Guariglia, per migliorare ancora la nostra collaborazione. E con un Paese afflitto da un atroce conflitto bellico, l'Ucraina, che ha ricevuto formazione dalla Scuola italiana e che è interessato ovviamente a rafforzare la sicurezza nazionale. Quindi, credo che la complessità del confronto che oggi è richiesto, che travalica sicuramente le fonti dell'Unione Europea, imponga di allargare l'ambito delle nostre riflessioni, avendo ormai ben chiaro che l'Intelligenza Artificiale si sviluppa su un terreno intrinsecamente interdisciplinare per le molte implicazioni etiche e filosofiche, ma anche per l'apporto sempre più marcato delle neuroscienze e, se necessario, della linguistica. Perché l'Intelligenza Artificiale si nutre di concetti e di parole, e questo serve a prevenire anche i crimini internazionali e a studiarne le implicazioni. Sappiamo tutti, proprio perché ci sono ormai tanti libri, veniva ricordato poco fa, che il mondo degli algoritmi è un mondo variegato, anche nell'applicazione ai sistemi giudiziari. Le implicazioni che più comprendiamo, perché forse sono anche più vicine a una pratica diffusa, sono le implicazioni che imprimono efficienza agli uffici, creazione di banche dati,

metodi sofisticati di archiviazione. Di tutto questo si parla nei corsi della scuola, ma dall'altro lato dobbiamo fronteggiare le sfide di algoritmi che apprendono per trasformare l'inazione in esperienza e, quello che più conta, in conoscenza. Non vi è un timore, perlomeno io mi sono rasserenata su questo fronte, ascoltando le rassicurazioni delle scienze fisiche e matematiche, non vi ha alcun timore di replicare la mente umana. Ma forse questo non basta per dare impulso ad una assiologia dell'Intelligenza Artificiale applicata ai sistemi giudiziari, soprattutto quando si affrontano temi legati alla prevenzione di crimini a rilevanza internazionale che sorgono e si sviluppano nello spazio virtuale. Il mio impegno personale e quello del comitato direttivo della Scuola Superiore della Magistratura è di rafforzare l'investimento nella formazione dei magistrati, tutti quelli italiani e non, perché molti non italiani transitano nelle nostre aule, con un'enfasi sempre più accentuata su aperture interdisciplinari per comprendere il ricorso all'Intelligenza Artificiale e le sue implicazioni. Ci proponiamo di farlo in un'ancora più proficua e feconda, se possibile, collaborazione con la Fondazione Vittorio Occorsio. La cultura dei magistrati deve espandersi nell'ascolto di altre voci, deve sempre più, lo è già, aprirsi alla contemporaneità in modo non acritico e, dunque, attingere alla conoscenza e al rispetto del pluralismo. La conoscenza del diritto è intessuta di dati, non soltanto tratti dalla vita materiale, ma anche di quelli che ora fluttuano nello spazio virtuale. Ricordo anche la stretta collaborazione con la Scuola Interforze qui a Roma. Le due Scuole hanno firmato una convenzione. Mi piace anche, e questo spero non sia un riferimento eclettico, ma lo faccio a beneficio anche degli ospiti stranieri che intervengono in questo convegno, ricordare che in Italia ci sono molteplici occasioni, e non da ora, già da anni, quindi tempo risalente, di confronto fra pensiero laico e pensiero religioso sui temi dell'Intelligenza Artificiale e sulle sue applicazioni alla giurisdizione. Si può ricordare l'esperienza del cosiddetto Cortile dei Gentili, che è un'occasione di grande livello di confronto fra laici e religiosi, che tra l'altro promuove dibattiti e pubblicazioni di grande interesse sui nostri temi. Ma lasciatemi citare un libro recente che ha un titolo accattivante: *L'algoritmo della vita*, che ha come sottotitolo *Etica e Intelligenza Artificiale*, scritto da Vincenzo Paglia, presidente della Pontificia Accademia per la Vita sta alimentando riflessioni sulle implicazioni etiche dei programmi di Intelligenza Artificiale. D'altronde, proprio a Roma nel 2020 c'è stata la *Rome Call for AI Ethics*, che è ispirata senz'altro ai valori sociali della Chiesa, ma promuove un monitoraggio interdisciplinare delle tecnologie e perfino un'etica transdisciplinare. Quindi non manca di valorizzare l'ambito giuridico perché si afferma la tutela delle persone. L'autore di questo libro esordisce con una citazione della Genesi che, da laica, vi ripropongo per porre l'accento sul lavoro come impe-

gno comune. Nella speranza che questi richiami non suonino, come ho detto prima, forse un po' estranei, addirittura eclettici rispetto agli altri temi di questo convegno, ma questo è un richiamo alto, perché nel Giardino di Eden l'uomo fu posto perché lo coltivasse e lo custodisse, e noi oggi guardiamo al lavoro dei magistrati e di quanti li affiancano nel contrastare e nel prevenire crimini internazionali, come a un lavoro che sta per spingersi nello spazio virtuale senza però mai perdere l'ancoraggio ai valori fondamentali, quelli che proprio sono piantati in questo giardino da custodire e coltivare.

APERTURA DEI LAVORI

Carlo Nordio
Ministro della Giustizia

Grazie dell'invito. Padrone di casa, ambasciatore Guariglia, Presidente, caro collega Giuseppe Amato, signori delle autorità. Naturalmente per primo, o come si dice ultimo ma non ultimo, Vittorio Occorsio. Anch'io vorrei iniziare questo breve intervento con un ricordo: quando Vittorio Occorsio, nonno, fu ucciso, io stavo sostenendo a Roma gli esami orali per entrare nella magistratura. Questo dimostra sia la mia età sia l'emozione con cui rievoco quell'episodio. Il presidente della commissione di allora, un grande giurista, si chiamava Mario, commentò che non saremmo arrivati a Natale, visto che ne avevano ammazzati tre in tre giorni. Questo lo dico perché il tributo che ha dato la magistratura, alla quale io mi sento ancora di appartenere, nella lotta al terrorismo e che ha in Vittorio Occorsio una delle sue figure più eminenti e significative, è un tributo che onora l'ordine al quale io appartenevo e al quale, ripeto, ancora oggi mi sento di appartenere, sia pure come Ministro.

Per quanto riguarda l'intervento di oggi, che come vedete è fatto a braccio, gli aspetti tecnici saranno molto più autorevolmente trattati rispetto alle scarse conoscenze, così direi 'cibernetiche', del sottoscritto, dello staff e degli appartenenti al nostro Ministero. Mi limiterei ad alcune considerazioni di ordine generale.

La prima riguarda il rapporto tra la legge e la tecnologia. L'uomo, nello spirito libero che lo contraddistingue, ha la capacità dell'invenzione. Per quanto riguarda la produzione normativa, noi tante volte ci troviamo in quello che il filosofo chiamava il paradosso di Achille e della tartaruga: mano a mano che Achille cerca di raggiungere la tartaruga, la tartaruga fa un passo avanti e Achille non la raggiungerà mai. Perché dico questo? Perché quando vi è una innovazione tecnologica, la legge molto spesso manca, e il legislatore è costretto a inseguire le problematiche che emergono dalla innovazione tecnologica. Questo è addirittura pericoloso nel sistema penale, per i vuoti di tutela che ci sono."

Tutti sappiamo che la legge penale non è retroattiva e quindi non è possibile incriminare un determinato comportamento se prima non era stato previsto dalla legge. Questo ci impone di lavorare di fantasia per comprendere quali saranno i problemi che l'innovazione tecnologica ci pone. Questo è accaduto sempre, anche nell'ambito del diritto civile. Basti pensare alle proble-

matiche sorte con la fecondazione artificiale, con i nuovi confini e i nuovi concetti della morte e della vita.

Una volta si pensava che la vita nascesse con la docimasia polmonare, oggi sappiamo che l'individuazione irreversibile del codice genetico di una persona avviene molto prima. Una volta si pensava che la morte coincidesse con l'arresto del battito cardiaco, oggi sappiamo che è l'elettroencefalogramma piatto a darci questa conoscenza, e che quindi si può anche procedere a cuore fermo. Tant'è vero che si fanno i trapianti. Voi tutti ricorderete quanto sia stato difficile, e ancora lo sia oggi, normare queste innovazioni tecnologiche, soprattutto nell'ambito del fine vita, proprio perché la tecnologia ci pone di fronte a problematiche che una volta erano impensabili.

E così è per la cyber security, così è per l'Intelligenza Artificiale. L'innovazione tecnologica, la telematica, la digitalizzazione, fino alla creazione di questa sorta di *monstrum*, che poi *monstrum* non è, dell'Intelligenza Artificiale, ha creato e crea problemi. Ma il messaggio con cui voglio iniziare, e tra poco concludere, questo intervento, è che noi dobbiamo convertire queste possibili criticità in opportunità.

Gli strumenti tecnologici non sono mai né buoni né cattivi, sono neutrali. Anche la fissione dell'atomo è neutrale: può creare una grande energia, ma può anche creare Hiroshima. La fusione nucleare è ancora più importante: se riuscissimo con la fusione nucleare a trasformare una bottiglia d'acqua in energia, potremmo illuminare l'intera città di Roma per 50 anni. Se invece la usiamo male, abbiamo l'esplosione di una bomba. Si chiamava Zar, e nel 1961 ebbe la potenza di 50 megatoni, cioè 50 milioni di tonnellate di tritolo, sufficienti a distruggere l'intera regione del Lazio.

E così è per l'Intelligenza Artificiale, e così per tutta la tecnologia. Se sappiamo usarla bene, avremo una grande opportunità; se la usiamo male, avremo l'inserimento di problematiche devastanti.

La presenza delle grandi organizzazioni criminali in quello che fino a ieri era soltanto un sistema di comunicazione, e che oggi invece è uno strumento di creazione di idee, ci pone davanti a nuove sfide. Ma anche qui dobbiamo fare attenzione a non confondere l'Intelligenza Artificiale con il cervello umano.

Ho assistito privatamente alla presentazione del libro citato dalla Presidente Sciarra, scritto da Monsignor Paglia, sull'algoritmo della vita, e mi onora l'amicizia del Cardinale Ravasi, che ha istituito il Cortile dei Gentili, anch'esso citato in precedenza. L'intelligenza umana, la capacità di distinguere non solo il logico dall'illogico, ma anche il bene dal male, è un tema radicato nella nostra cultura. È scritta nella Bibbia. La Presidente Sciarra ha menzionato il Giardino dell'Eden. Se leggiamo la Genesi, vediamo che, quando

Adamo mangia il frutto proibito, Dio dice: "Ecco, è diventato come uno di noi, perché conosce la differenza tra il bene e il male."

Mangiare il frutto proibito è una rappresentazione mitologica dell'evoluzione dell'intelligenza umana. Questa evoluzione ha distinto l'uomo dall'animale, perché prima, non sapendo distinguere il bene dal male, l'uomo – o meglio, quella creatura che forse non era nemmeno uomo – era simile a un animale, a un vegetale. Se non sai distinguere il bene dal male, non puoi scegliere né l'uno né l'altro e sei privo di autonomia morale. Non sei un essere morale, ma un essere indifferenziato. E lì è nata l'intelligenza, lì è nata la moralità, l'etica.

Noi siamo monopolisti inclusivi di questa intelligenza. Non esiste la possibilità che un'Intelligenza Artificiale possa sostituirsi o surrogarsi all'intelligenza umana. L'Intelligenza Artificiale è un prodotto dell'uomo, così come lo sono gli algoritmi e, in futuro, lo saranno gli algoritmi degli algoritmi. Potranno replicare, ma non creare; sarebbe una creazione fittizia.

Credo che con l'Intelligenza Artificiale si possa, ad esempio, ricostruire con nuovi accordi una suite di Bach, mantenendo gli stessi rapporti tra le armonie delle varie sezioni e sequenze. L'Intelligenza Artificiale potrebbe creare una settima suite per violoncello solo, ma non sarebbe una suite di Bach. Sarebbe una replica, simile a quella che i madonnari realizzano sui pavimenti del Duomo: copie di Michelangelo, ma non Michelangelo stesso. Sono semplicemente un *copia e incolla* con una dimensione diversa rispetto all'originale.

Dall'intelligenza umana e dalle libertà dello spirito deriva la conclusione alla quale vorrei arrivare: non dobbiamo avere paura della nuova cyber-innovazione e, in particolare, dell'Intelligenza Artificiale. Sono creature nostre, che devono essere gestite dal cervello e, soprattutto, dal cuore umano.

Il primo a inventare una sorta di Intelligenza Artificiale, un piccolo cervello elettronico, cioè una piccola calcolatrice, fu niente meno che un grande filosofo: Blaise Pascal. Egli costruì la prima calcolatrice, che ancora oggi si chiama "pascalina". Questo stesso filosofo e scienziato scrisse uno dei più bei pensieri della storia della filosofia: l'essere umano è dotato di uno *esprit de géométrie* e di uno *esprit de finesse*. Lo *esprit de géométrie* riguarda il cervello, la logica; lo *esprit de finesse* riguarda il cuore, l'etica.

Se riusciamo a coniugare entrambe queste possibilità, come voleva Pascal, allora l'Intelligenza Artificiale non sarà un pericolo, ma una grande opportunità.

Giovanni Salvi

Presidente del Comitato Scientifico FVO, già Procuratore generale presso la Suprema Corte di Cassazione

Il mio intervento è un fuori programma, che spero possa essere utile per introdurre i nostri due prossimi oratori che ci parleranno degli aspetti più avanzati dell'Intelligenza Artificiale, emersi nel percorso del G7 a guida giapponese e poi nel lavoro del Gruppo *UK Frontier AI*, in maniera che da questo approccio possano poi trarsi, nei successivi lavori, le conseguenze per il nostro specifico campo di lavoro. Il focus dei nostri lavori, in realtà, nel maremagnum di questioni che si pongono nel cyber, è concentrato su di un tema molto specifico, peraltro già introdotto dal Ministro Nordio e dal Procuratore Generale Amato: il ruolo della giurisdizione in questa nuova sfida e il suo rapporto con altre forme di poteri sovrani.

La giurisdizione non come meramente affermata, perché qualunque Stato può affermare la propria giurisdizione universale; renderla poi effettiva è tutt'altra cosa, soprattutto in una situazione che vede anche altri attori. È vero che la giurisdizione è fondamentale, e lo vedremo nello sviluppo di tutto questo lavoro, ma renderla effettiva vuol dire anche rapportarsi ad altri attori, che ormai in questo settore sono coloro che operano di fatto efficacemente: dalla resilienza, nel nostro caso l'Autorità Nazionale per la Cyber Sicurezza, al settore dell'Intelligence, che ha ormai una importanza rilevantissima.

Avremmo dovuto avere oggi il Procuratore Nazionale Antimafia, Giovanni Melillo. Purtroppo, per ragioni serie e personali, nei giorni passati ha dovuto rinunciare, e quindi questa assenza ha fatto venire meno l'introduzione ai molti problemi che si affrontano nel rapporto tra resilienza, Intelligence e giurisdizione, anche a seguito delle recenti modifiche normative in Italia e dei molti interventi regolatori sovranazionali, in essere o in discussione. E quindi io cerco, immodestamente, di dare qualche indicazione su alcuni di questi aspetti, per spiegare il senso della successione delle relazioni nel seminario. Poi abbiamo qui il Procuratore nazionale aggiunto, Michele Prestipino, che, se vorrà intervenire al termine delle presentazioni, ci farà un grande regalo.

Quindi, transnazionalità intrinseca al cybercrime. I cybercrimes più gravi possono riguardare strutture critiche di una nazione. Negli ultimi anni le maggiori infrastrutture di alcuni Paesi sono state oggetto di attacchi di varia natura, e nessuna di esse può considerarsi al sicuro. Per esempio, gli attacchi più frequenti e i più gravi sono avvenuti nei confronti della sanità, infrastruttura tra le più critiche per la sicurezza nazionale.

Le crescenti capacità di evolversi autonomamente da parte degli strumenti offensivi che si basano sull'Intelligenza Artificiale di frontiera rendono

questi attacchi sempre più efficaci e le contromisure sempre più difficili.

Il G7 a guida giapponese ha prodotto, nell'anno passato, due importanti risultati circa le sfide imminenti della AI e la necessità di un approccio globale a queste sfide. L'*Hiroshima Process on AI*, affronta i temi della difesa dagli attacchi cibernetici e delle sue implicazioni circa il dislocarsi dei poteri e delle garanzie. Di questo processo ci parlerà la dr.ssa Keiko Kono, che vi ha preso parte.

L'approccio finalizzato alla regolazione da parte della Comunità internazionale ha poi avuto uno sviluppo nel lavoro del Gruppo organizzato dalla Gran Bretagna e che ha prodotto, alla fine del 2023, un importante elaborazione, sempre in ambito G7, condensata nel documento *UK AI Frontier*, che analizza lo stato attuale della Intelligenza Artificiale "di frontiera", la sua imprevista velocità di sviluppo e le nuove prospettive, per i prossimi anni.

Il quadro etico, regolartorio e tecnico che emerge dal complesso di queste iniziative è indispensabile per porre la discussione sulla effettività della giurisdizione nello Spazio Virtuale su basi di realtà, sfuggendo alle facili impostazioni prescrittive: ad esempio, lo *Human in the Loop* è certamente un imperativo etico e può essere trasfuso in norme, ma come renderle effettivamente vincolanti nella transnazionalità?

Per queste ragioni, il seminario si apre con una rassegna di queste acquisizioni da parte di ricercatori che hanno partecipato a quei lavori. Avremmo dovuto avere il vicedirettore dell'Istituto britannico; anche lei, purtroppo, ha avuto serie ragioni di salute nei giorni passati, per le quale le rivolgiamo caldi auguri, e quindi non ci sarà, ma è degnamente sostituita dal tenente colonnello Massimiliano Signoretti, che a lungo si è occupato di queste materie.

Le operazioni malevole condotte con strumenti informatici avanzati, in realtà, rilevano contemporaneamente per diversi aspetti che attengono alla sovranità nazionale. Un attacco informatico rivolto alle strutture critiche è innanzitutto un delitto, secondo le previsioni della maggior parte dei Paesi, e la Convenzione sul Cybercrime delle Nazioni Unite, il cui testo finale sarà in discussione nei prossimi mesi nell'Assemblea Generale, fornirà un ulteriore catalogo di questi delitti che diventeranno, quindi, riconosciuti in forme condivise dalla maggior parte dei Paesi del mondo.

Tali operazioni richiedono al tempo stesso una reazione dello Stato attaccato volta a ridurre il danno e a prevenire danni futuri, che è l'attribuzione tipica delle strutture di resilienza, come la nostra ANC.

Gli attacchi, infine, costituiscono una violazione della sovranità e, nei casi più gravi, legittimano forme di reazione che possono giungere fino alla risposta cinetica contro lo Stato cui l'azione è attribuita.

I tre livelli dell'operazione malevola interferiscono tra di loro e richie-

dono, quindi, un serio coordinamento, innanzitutto a livello nazionale. Interventi normativi recenti in Italia hanno esteso i poteri di azioni volte alla resilienza e alla prevenzione attiva, nonché alla risposta offensiva. Questa, attribuita alle Agenzie di Intelligence, è stata rafforzata. La possibilità di ricorrere a operazioni sottocopertura, di infiltrazione nelle strutture informatiche attaccanti, è poi attribuita tanto alle forze di polizia, con l'autorizzazione dell'autorità giudiziaria, quanto all'Intelligence.

Tra i problemi che tali novità pongono vi è dunque il rapporto tra i tre livelli della reazione, per far sì che essi non interferiscano tra loro, finendo per ostacolarsi a vicenda. Centrale dal punto di vista della giurisdizione è il ruolo ora svolto dalla Procura Nazionale Antimafia e Antiterrorismo. Tuttavia, le potenziali interferenze sono molto ampie. In realtà, alcune delle principali operazioni che hanno consentito di debellare strutture criminali come le cripto piattaforme sono frutto non di decriptazione di algoritmi, ma di operazioni combinate nelle quali l'Intelligence ha svolto un ruolo significativo, forse centrale. Quindi, quello che a noi era sembrato un'operazione di rottura della criptazione degli algoritmi, in realtà spesso ha avuto alla base un'operazione tradizionale di intelligence e di penetrazione.

La raccolta della prova da utilizzarsi nel processo penale, di conseguenza, non incontra solo il tema della leggibilità posteriore dell'algoritmo. Il tema diventa anche quello della prova proveniente dall'Intelligence. A seconda dei sistemi processuali, queste prove potranno essere ammissibili o meno, seguendo comunque iter differenziati. Si tratta di un tema che va ad aggiungersi a quello tradizionalmente affrontato nelle aule di giustizia della trasparenza delle operazioni di decrittazione.

La giurisdizione deve affrontare la difficoltà derivante dalla transnazionalità delle operazioni, ulteriormente caratterizzate nel nostro specifico da volatilità, opacità, non localizzazione e logica non deterministica.

Ciò implica che i meccanismi di collaborazione internazionale, basati sul consenso successivo degli Stati all'acquisizione della prova, sono di fatto inefficaci. Presto entreranno in vigore le nuove fondamentali disposizioni europee sulle acquisizioni di prova elettronica. Ma le difficoltà nella raccolta delle prove sono comuni ai diversi sistemi ordinamentali. Gli Stati Uniti, che lavorano da molti anni su questo, hanno già da tempo predisposto uno strumento normativo per superare alcune di queste difficoltà: il *Cloud Act*. Esso tenta di superare il difficile ostacolo costituito dalla reale dislocazione dei poteri nello spazio virtuale tra Stati nazionali, istituzioni sovranazionali e grandi gruppi privati.

I grandi gruppi privati operano nello Spazio Virtuale come una sorta di nuova Compagnia delle Indie, esercitano di fato poteri regolatori e autoritati-

vi che un tempo erano prerogativa dello Stato nazionale, anzi il terreno privilegiato in cui si manifestava la caratteristica essenziale di questo, la sovranità. Se il partenariato è ormai indispensabile, ciò non toglie che l'esercizio della giurisdizione, almeno per le sue intrinseche caratteristiche nello Stato di diritto, non può essere condizionato dal consenso di chi esercita di fatto quei poteri.

Anche la modifica della *Rule 41* della *Federal Rules of Criminal Procedure* negli Stati Uniti non ha consentito di risolvere questo problema per le attività che si svolgono all'estero, ma esclusivamente all'interno, cercando di prevenire che vi siano vittime addizionali dei crimini. I poteri del *Law Enforcement*, tuttavia, anche a seguito di quella modifica, restano confinati nella giurisdizionale nazionale, consentendo il superamento della frammentazione tra gli Stati federati.

La conseguenza è che l'obiettivo del Dipartimento di Giustizia, secondo le indicazioni provenienti dalla *Deputy Attorney General* Lisa Monaco, competente per materia, è di combattere il cyber crime incrementando la priorità della *disruption*, non più quella della condanna di coloro che all'estero svolgono queste attività, ritenuta di fatto non praticabile. Questo approccio, reso possibile dalla duttilità dell'ordinamento statunitense, non sarebbe immaginabile nel nostro ordinamento, perché trasformerebbe radicalmente il sistema penale.

Nel nostro ordinamento, questa attività è attribuita all'Intelligence. L'attività giudiziaria è secondaria e di risulta, perché nel tentare di identificare e portare a punizione i responsabili, abbiamo anche la possibilità di svolgere questi ruoli di prevenzione.

In conclusione, tutto questo ci porta alle similitudini e alle differenze tra le attività dell'Intelligence e quelle della giurisdizione. Questo è ciò che ci verrà spiegato da coloro che, conoscendo questi nuovi meccanismi, possono illustrarci perché è estremamente difficile seguire, nello spazio sovranazionale e in più Paesi, le tracce di un'aggressione, assicurando al contempo che la prova sia in forme legittimamente utilizzabili in un processo penale. Problemi, questi, analoghi a quelli che si incontrano nel diritto pubblico internazionale a proposito del principio di attribuzione, Questi sono i gravi temi che noi vorremmo affrontare, non dico risolvere, nello sviluppo di questi due giorni di lavoro. Partire dalla consapevolezza che questa sfida è diversa da quelle affrontate in passato: raggiungere la prova, raccogliere la prova e renderla soprattutto utilizzabile nel processo penale, quindi in un contraddittorio tra le parti, nelle quali il segreto o non può entrare, o entra con modalità tali da garantire comunque i diritti delle parti. Far funzionare questi meccanismi comporta una chiara disciplina dei rapporti tra l'Intelligence, la resilienza e la

giurisdizione, e la capacità di comprendere che la giurisdizione oltre un certo punto non riuscirà ad arrivare, e che l'Intelligence dovrà comunque rispettare, come già avviene nel nostro ordinamento, i principi fondamentali dello Stato di diritto.

Con questa premessa, spero di aver dato il senso di quanto ascolteremo adesso, che sarà un'illustrazione delle novità nell'ambito dell'intelligenza artificiale di frontiera. Molte grazie.

RELAZIONE INTRODUTTIVA SULLE NUOVE FRONTIERE DELL'IA (A PARTIRE DAL PROCESSO G7 – HIROSHIMA AI) E SUI LORO EFFETTI SULLA SOVRANITÀ NAZIONALE E L'EFFICACIA DELL'ESERCIZIO DELLA GIURISDIZIONE

Keiko Kono
Esperta del Processo AI di Hiroshima

È un grande onore presentare oggi il G7 *Hiroshima AI Process*. Con l'avvento dell'IA generativa, i criminali non hanno più bisogno di esperti tecnici come in passato per portare a termine i cyberattacchi. Chiunque può scrivere sofisticate e-mail di *phishing*, creare *malware* e contenuti *deepfake* utilizzando la tecnologia dell'IA generativa. L'efficienza del loro lavoro è quindi notevolmente migliorata grazie alla tecnologia AI. Di conseguenza, la difesa contro questi crimini informatici e operazioni informatiche abilitati dall'IA sta diventando ancora più impegnativa in termini di velocità e scala. Il processo di *Hiroshima AI* del G7 è stato lanciato lo scorso anno con l'obiettivo di promuovere la sicurezza, la protezione e l'affidabilità dei sistemi avanzati di IA e di contribuire a ridurre questi rischi. Spero che i risultati dell'*Hiroshima AI Process* che presenterò oggi siano rilevanti e contribuiscano alla discussione di questa conferenza.

Inizio la presentazione con la cronologia del Processo di Hiroshima. Quindi, introduco brevemente il documento principale dei risultati del Processo di Hiroshima sull'IA, ovvero il Codice di Condotta Internazionale per gli Sviluppatori di IA Avanzate del Processo di Hiroshima, compreso il suo meccanismo di monitoraggio. Infine, concludo con alcune questioni in sospeso che si prospettano con l'obiettivo di sviluppare un quadro di governance dell'IA a livello globale.

Durante le riunioni del G7 del 2022, l'Intelligenza Artificiale non era particolarmente all'ordine del giorno. Tuttavia, nel 2023 è diventata improvvisamente uno dei temi principali delle riunioni dei ministri del digitale e della tecnologia, dopo la pubblicazione del GPT-4 nel marzo 2023. Nel maggio 2023, i leader del G7 hanno annunciato l'avvio del Processo di Hiroshima sull'IA per discutere le priorità politiche comuni relative all'IA generativa. Il mese successivo, il Gruppo di lavoro del G7 ha iniziato i suoi lavori su iniziativa del governo giapponese, che ha distribuito un questionario ai membri del G7 per fare il punto sulle opportunità e le sfide delle tecnologie di IA generativa. Sulla base dei risultati del questionario, il gruppo ha redatto dei docu-

menti finali in collaborazione con esperti esterni, tra cui l'OCSE. Il lavoro di redazione si è concluso intorno al 9 ottobre e alla fine dello stesso mese i leader del G7 hanno pubblicato due documenti. Uno è costituito dai Principi guida internazionali e l'altro dal Codice di condotta internazionale. Entrambi i documenti sono destinati alle organizzazioni che sviluppano IA avanzata. Il 1° dicembre, i ministri del digitale e della tecnologia del G7 hanno concordato il "Quadro globale del processo di Hiroshima sull'IA", dopo aver incorporato il feedback di un'indagine condotta dalle parti interessate nell'UE, in Giappone e negli Stati Uniti. Il quadro politico globale è stato approvato in una dichiarazione dei leader cinque giorni dopo. Nel 2024, la governance dell'IA rimane all'ordine del giorno delle riunioni del G7 sotto la presidenza italiana.

A maggio, in occasione di un evento dell'OCSE, l'allora primo ministro giapponese Kishida ha annunciato la creazione del Gruppo di amici del processo di Hiroshima, con la partecipazione di Paesi non appartenenti al G7. Attualmente, 53 Paesi e l'Unione Europea fanno parte dell'elenco, come mostrato nella diapositiva. Inoltre, l'elenco degli sviluppatori di IA "che si impegnano ad attuare il Codice di condotta internazionale del Processo di Hiroshima" sarà pubblicato successivamente sullo stesso sito web del Processo di Hiroshima.

Il 19 luglio 2024, l'OCSE ha lanciato la fase pilota del *Reporting Framework for the International Code of Conduct for Organizations Developing Advanced AI Systems* e ha invitato alla partecipazione volontaria online. La scadenza era il 6 settembre e i risultati dell'indagine dovrebbero essere pubblicati successivamente sullo stesso sito web. Mi aspetto che ulteriori dettagli, compreso il lancio ufficiale del *Reporting Framework*, vengano decisi in occasione della prossima riunione ministeriale su Industria, Tecnologia e Digitale del 15 ottobre.

Come risultato del Processo di Hiroshima sull'IA, è stato presentato il "Quadro politico globale del Processo di Hiroshima sull'IA" con i seguenti quattro elementi: (1) il rapporto dell'OCSE "Verso un'intesa comune del G7 sull'IA generativa", (2) i principi guida internazionali per tutti gli attori dell'IA, (3) il codice di condotta internazionale per gli sviluppatori di IA e (4) la cooperazione basata su progetti sull'IA, che prevede la cooperazione con progetti e iniziative esistenti e nuovi sull'IA generativa in tutto il mondo.

Il rapporto dell'OCSE include i risultati del questionario inviato ai membri del G7 per identificare le priorità politiche comuni per l'IA generativa. Il rapporto mostra che tutti i membri del G7 considerano la "disinformazione e la relativa manipolazione delle opinioni" come il rischio dominante.

In termini di cyber, i 3 Paesi hanno considerato come rischio rispettivamente "minacce alla sicurezza informatica" e "minacce alle attività illegali". [1]

E tutti i membri del G7 ritengono che l'uso "responsabile" delle tecnologie di IA generativa sia la priorità più URGENTE e IMPORTANTE dal punto di vista politico.

Il successivo lavoro di discussione e stesura del gruppo di lavoro è stato condotto tenendo conto di questo risultato del questionario.

Il secondo e il terzo punto del Quadro politico globale hanno un contenuto quasi identico, poiché il Codice di condotta è una versione più elaborata dei Principi guida. L'unica differenza tra i due è il pubblico a cui sono destinati. I Principi guida sono destinati a tutti gli utenti dell'IA, con 12 principi, 11 dei quali ripresi dai Principi guida per gli sviluppatori di IA pubblicati a ottobre. È stato aggiunto un nuovo principio per tutti gli attori dell'IA, che li invita a "promuovere e contribuire all'uso affidabile e responsabile dei sistemi avanzati di IA".

Per motivi di tempo, oggi discuterò solo del Codice di Condotta. La diapositiva mostra l'elenco delle azioni e delle raccomandazioni contenute nel Codice di condotta, che le organizzazioni che sviluppano l'IA dovrebbero seguire.

1. Identificazione, valutazione e gestione dei rischi dell'IA (*) prima dell'implementazione

Azione n. 1: le organizzazioni devono "*adottare misure appropriate durante lo sviluppo di sistemi avanzati di IA ..... per identificare, valutare e mitigare i rischi lungo tutto il ciclo di vita dell'IA*". Tali rischi dell'IA comprendono le capacità informatiche offensive e le minacce ai valori democratici e ai diritti umani, tra cui l'agevolazione della disinformazione o la violazione della privacy. A tal fine, le organizzazioni dovrebbero impiegare una serie di misure di verifica interne ed esterne.

2. Monitoraggio e rendicontazione post-impiego

Azione n. 2: le organizzazioni devono "*identificare e mitigare le vulnerabilità ..... dopo l'implementazione"* attraverso il rilevamento e la segnalazione di terze parti e degli utenti.

---

1 D: Quali sono i cinque principali rischi che l'IA generativa presenta per il raggiungimento degli obiettivi nazionali e regionali? (Figura 2.2 nel rapporto dell'OCSE).

3. Rendicontazione per la trasparenza

Azione n. 3: le organizzazioni dovrebbero *"comunicare pubblicamente le capacità, le limitazioni e gli ambiti di utilizzo appropriato e inappropriato dei sistemi avanzati di IA, al fine di garantire una sufficiente trasparenza, contribuendo così ad aumentare la responsabilità"*. Esempi di tali misure sono i rapporti di trasparenza.

4 Gestione e segnalazione degli incidenti

Azione n. 4: Le organizzazioni devono "*lavorare per una condivisione responsabile delle informazioni e per la segnalazione degli incidenti ..... con l'industria, i governi, la società civile e il mondo accademico"*.

5. Governance organizzativa

Azione n. 5: le organizzazioni dovrebbero *"sviluppare, implementare e divulgare le politiche di governance e di gestione del rischio dell'IA"* e migliorare la familiarità dei dipendenti con i loro doveri.

6. Sicurezza delle informazioni

Azione n. 6: le organizzazioni devono *"investire e implementare solidi controlli di sicurezza, tra cui la sicurezza fisica, la cybersecurity e le protezioni contro le minacce interne lungo tutto il ciclo di vita dell'IA"*.

7. Autenticazione e provenienza dei contenuti

Azione n. 7: le organizzazioni dovrebbero *"sviluppare e implementare meccanismi affidabili di autenticazione e provenienza dei contenuti, ove tecnicamente possibile, come il watermarking ..... per consentire agli utenti di identificare i contenuti generati dall'Intelligenza Artificiale*".

8. Ricerca e investimenti per migliorare la sicurezza dell'IA e mitigare i rischi per la società

Azione n. 8: le organizzazioni devono *"dare priorità alla ricerca per mitigare i rischi per la società, la sicurezza e l'incolumità e dare priorità agli investimenti in misure di mitigazione efficaci"*, il che include la ricerca sul sostegno dei valori democratici, il rispetto dei diritti umani, la protezione dei bambini e dei gruppi vulnerabili, la salvaguardia della proprietà intellettuale e della privacy e la prevenzione di pregiudizi dannosi, disinformazione, disinformazione e manipolazione delle informazioni.

9. Promuovere gli interessi umani e globali

Azione n. 9: le organizzazioni dovrebbero *"dare priorità allo sviluppo di sistemi avanzati di IA per affrontare le maggiori sfide del mondo",* tra cui la crisi climatica, la salute globale e l'istruzione.

10. Interoperabilità e standard internazionali

Azione n. 10: le organizzazioni sono incoraggiate a *"far progredire lo sviluppo e, ove appropriato, l'adozione di standard tecnici internazionali"* e delle migliori pratiche, anche per quanto riguarda il *watermarking.*

11. Misure di inserimento dati e protezione dei dati personali e della proprietà intellettuale

Azione n. 11: le organizzazioni sono incoraggiate a *"implementare misure appropriate di inserimento dei dati* [per mitigare i pregiudizi dannosi] *e protezioni per i dati personali e la proprietà intellettuale".* Come molti di voi sapranno, altre iniziative di governance dell'IA sono state avviate parallelamente al Processo di Hiroshima sull'IA nel 2023. In particolare, l'OCSE ha pubblicato l'aggiornamento dei "Principi sull'IA" nel maggio[2] e il governo degli Stati Uniti ha annunciato "Impegni volontari da parte delle principali aziende di IA per gestire i rischi posti dall'IA" nel luglio.[3] Non so quale sia stata la discussione all'interno del gruppo di lavoro, che ha richiesto oltre 100 ore, ma data la somiglianza tra questi documenti, sembra che il lavoro di stesura del Codice di Condotta del Processo di Hiroshima sia stato ispirato o almeno infuso con le idee dei Principi di IA dell'OCSE e degli Impegni Volontari delle principali aziende americane di IA, come mostrato nella slide.

Come ho spiegato in precedenza, da luglio a settembre l'OCSE ha condotto la fase pilota del quadro di rendicontazione del Codice di condotta internazionale per le organizzazioni che sviluppano sistemi avanzati di IA. L'indagine ha lo scopo di "monitorare l'applicazione volontaria del Codice di condotta da parte degli sviluppatori di IA ed è strutturata intorno agli 11 punti d'azione del Codice di condotta, per un totale di 48 pagine". Oltre ai membri del Gruppo di lavoro del G7 e agli esperti dell'OCSE, alla stesura delle

---

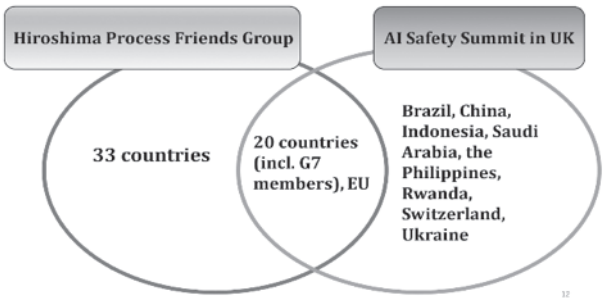
2 AI Principles Overview - OECD.AI

3 Il 23 luglio 2023, SCHEDA INFORMATIVA: L'amministrazione Biden-Harris ottiene impegni volontari da parte delle principali aziende di intelligenza artificiale per gestire i rischi posti dall'IA | La Casa Bianca

domande del sondaggio hanno partecipato aziende e organizzazioni di IA dei Paesi del G7.[4]

Nel complesso, il Codice di condotta del processo di Hiroshima avrà probabilmente un impatto positivo sul modo in cui le aziende di IA gestiscono il rischio nei loro prodotti durante l'intero ciclo di vita dell'IA. I documenti del Processo di Hiroshima sono un processo continuo e sono destinati a essere flessibili, in quanto continueranno a essere rivisti e aggiornati in base ai progressi della tecnologia e all'evoluzione delle politiche.[5]

Tuttavia, sembravano esserci diverse questioni in sospeso che dovevano essere affrontate. In primo luogo, come affermato nella Dichiarazione dei Ministri del Digital & Tech del dicembre 2023, il coordinamento e la cooperazione tra i forum multilaterali[6] sono fondamentali per raggiungere l'obiettivo fissato dal Processo di Hiroshima sull'IA, che è quello di promuovere la sicurezza, la protezione e l'affidabilità dei sistemi avanzati di IA a livello internazionale. Il gruppo consultivo di alto livello delle Nazioni Unite sull'IA ha notato che più di 100 Paesi non hanno partecipato a nessuna delle recenti iniziative di governance dell'IA e ha suggerito che "è necessario un forum politico inclusivo in modo che tutti gli Stati membri ..... possano condividere le migliori pratiche".[7] Il Processo di Hiroshima sull'IA deve cogliere l'opportunità di raggiungere un maggior numero di Paesi.



4 Canada: Cohere/France: Mistral AI/Germany: German Research Center for AI (DFKI)/Italy: iGnenius/Japan: Nippon Telegraph and Telephone Corporation (NTT), Nippon Electric Company (NEC)/US: Microsoft, Google, AWS, Meta, Open AI, Anthropic. G7、AI悪用リスクを監視　健全な活用へ世界共通基準 - 日本経済新聞 (nikkei.com) 2024年9月15日、

5 Para. 9, https://www.soumu.go.jp/hiroshimaaiprocess/pdf/document02_en.pdf

6 Para. 11, ibid.

7 The UN high-level Advisory Body on AI, "Governing AI for Humanity: Final Report," 2024, p, 52, paras. 103-104, https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_en.pdf

Un esempio di queste iniziative esistenti è il Vertice sulla sicurezza dell'IA avviato dal governo britannico lo scorso anno. Come mostrato nella diapositiva, 8 Paesi che partecipano al Vertice sulla sicurezza dell'IA del Regno Unito non sono ancora membri del Gruppo di amici del processo di Hiroshima.

Infine, è importante tenere tutte le parti interessate ben informate sui rischi comuni dell'IA e promuovere una comprensione il più possibile comune a livello internazionale. Ad esempio, la pedopornografia *deepfake* è un crimine informatico in alcuni Paesi, ma non in altri, anche se questi ultimi hanno aderito alla Convenzione di Budapest sulla criminalità informatica. In questo caso, la percezione del rischio del *deepfake* può variare da Paese a Paese. E questi contenuti orribili circoleranno per sempre su Internet. Da un lato, spetta ai singoli Paesi decidere se criminalizzare o meno determinati reati, ma dall'altro non conosciamo ancora il quadro generale della tecnologia AI generativa. I documenti dell'*Hiroshima AI Process* adottano un approccio basato sul rischio. Ciò significa che il quadro di governance dell'IA potrebbe cambiare a seconda della percezione del rischio in futuro. Pertanto, tenendo conto di questi cambiamenti, la discussione su quale sia il giusto equilibrio tra opportunità e rischi dovrebbe continuare.

Massimiliano Signoretti
Tenente Colonello Aeronautica Militare, consulente giuridico Comando Operazioni in Rete, Stato Maggiore della Difesa

Grazie molte per questa opportunità di intervenire in questo prestigioso evento. Mi sostituisco alla dottoressa Imogen Schon, *deputy director* del *Safety Institute* del Ministero della Scienza, Innovazione e Tecnologia del Regno Unito. Inizio parlando di un approccio all'Intelligenza Artificiale e alle nuove frontiere tecnologiche che è innovativo rispetto ad altri.

L'approccio del Regno Unito si distingue da quello dell'Unione Europea. Non si focalizza tanto su un'immediata regolamentazione dei sistemi di Intelligenza Artificiale e del loro utilizzo, quanto sul governare e controllare la traiettoria di un fenomeno dirompente nella vita dei cittadini. Questo approccio prevede la costituzione di una *Task Force* di esperti di Intelligenza Artificiale a livello mondiale, con il ruolo iniziale di board consultivo all'interno di una struttura governativa. Questo *board* si evolve successivamente in un *High Safety Institute*, che definisce un approccio volto alla comprensione e al governo delle potenzialità e dei rischi.

Si parte dalla constatazione che non abbiamo piena conoscenza delle possibilità di sviluppo dei nuovi modelli di Intelligenza Artificiale. Applicazioni note come ChatGPT o GPT-4 illustrano solo una parte delle sue capacità. Personalmente, ho trovato strumenti come Gamma AI straordinari, ad esempio, per creare slide e presentazioni in tempi ristretti. Governare tali applicazioni significa partire dal riconoscere che l'Intelligenza Artificiale non è solo negativa: presenta vantaggi enormi, come la prevenzione precoce di alcune patologie e lo sviluppo di calcoli quantistici.

Tuttavia, esistono anche rischi significativi, come la capacità di Intelligenza Artificiale e *quantum computing* di rompere codici crittografici entro 5-10 anni. Questo crea fenomeni come il *data harvesting*, con la sottrazione massiva di dati da banche dati per un futuro in cui tali informazioni potranno essere decriptate. L'approccio del Regno Unito mira anche a sfruttare le potenzialità di queste tecnologie attraverso l'istituzione di laboratori di test e valutazione, concentrando a livello governativo la capacità di comprendere e governare i rischi.

In questo contesto, la DARPA, agenzia statunitense di ricerca avanzata per la difesa, ha classificato lo sviluppo dell'Intelligenza Artificiale in tre ondate. La prima si basa sull'apprendimento da grandi moli di dati per generare output; la seconda utilizza algoritmi probabilistici; la terza, in corso, riguarda l'adattamento ai contesti, con sistemi in grado non solo di apprendere ma di comprendere relazioni tra dati, influenzando decisioni e processi.

Guardando al panorama internazionale, emerge un approccio duale: sfruttare le opportunità dell'Intelligenza Artificiale e governarne i rischi. La NATO, ad esempio, ha già emanato strategie specifiche, aggiornate nel 2024 con la creazione dell'agenzia DIANA (*Defence Innovation Accelerator for the North Atlantic*) per accelerare le conoscenze in campo tecnologico. Anche l'Unione Europea ha adottato regolamentazioni, classificando l'Intelligenza Artificiale in base ai rischi e vietando applicazioni che compromettono i diritti fondamentali, come la profilazione degli individui.

Un tema centrale è la sovranità. Il diritto internazionale è fortemente legato al principio di territorialità e i comportamenti degli Stati, specie con capacità autonome, possono violarlo. Il Manuale di Tallinn esplora come il diritto internazionale si applica alle operazioni cyber, identificando tre tipi di illecito: l'ingresso fisico in un sistema, l'accesso da remoto e l'interferenza politica, quest'ultima particolarmente critica per i suoi effetti sulle elezioni e sulle decisioni politiche.

L'impiego di capacità autonome e Intelligenza Artificiale pone problemi significativi, soprattutto nel determinare il collegamento tra operazioni cyber e responsabilità statali. Elementi psicologici, come l'intenzione di interferire negli affari interni di un altro Stato, complicano ulteriormente l'attribuzione delle responsabilità.

A livello normativo, spesso le capacità di Intelligenza Artificiale destinate a scopi militari o di sicurezza sono escluse dalla regolamentazione generale, sia nell'Unione Europea che a livello nazionale. Tuttavia, tali esenzioni devono rispettare i diritti fondamentali e i principi costituzionali.

Infine, il Comitato Internazionale della Croce Rossa non si oppone totalmente all'uso di capacità autonome nei conflitti armati, purché siano rispettati principi come necessità, distinzione e precauzione. Ad esempio, richiede il mantenimento del controllo umano e l'implementazione di *kill switch* per interrompere operazioni quando i principi umanitari sono a rischio. Anche il *geofencing* e la prevenzione della propagazione indiscriminata del software sono requisiti essenziali.

DIBATTITO

Massimiliano Signoretti:

Se ci sono domande, sono ben lieto di poter rispondere, di cercare di rispondere.

Giovanni Salvi:

Grazie. È molto interessante la presentazione del Colonnello Signoretti sul punto relativo all'utilizzo di strumenti che comunque richiedano la presenza dell'uomo ma che siano in grado di autodeterminarsi in situazioni di conflitto. Non pensa che il serio problema sia che debba essere bilaterale questa situazione? Perché, se uno dei due operatori non utilizza strumenti controllabili, quindi perdendo una parte consistente del vantaggio – perché il vantaggio è proprio nella non esistenza dell'intervento umano che consente di sfruttare la grande rapidità di decisione e la maggiore precisione di decisione rispetto a quella umana dello strumento artificiale – ecco, la presenza dell'obbligo dell'intervento umano rende meno competitivo. Questo, in una situazione di conflitto, non determinerà, come già è successo nelle guerre precedenti, un fortissimo aumento invece dell'utilizzo di questi strumenti? Sono stato chiaro?

Massimiliano Signoretti:

Sì, dottor Salvi. Sì, questo è sicuramente un problema. È un problema che però parte da prima dell'impiego di queste capacità autonome in un teatro operativo; parte dal momento in cui noi concepiamo e addestriamo le capacità cyber autonome, in cui addestriamo l'intelligenza artificiale. Perché quando noi addestriamo queste capacità, inseriamo all'interno delle istruzioni sostanzialmente, che vengono fornite a questi sistemi, i codici e i limiti che ci derivano dal far parte di sistemi democratici.

Quindi è vero che poi ci confrontiamo, eventualmente, con Paesi che non hanno questa attenzione a integrare, all'interno dell'addestramento dei loro sistemi di intelligenza artificiale, i principi democratici e i valori fondamentali. Ma su questo non credo che possiamo in ogni caso transigere, e quindi dobbiamo in qualche modo cercare di colmare questo gap, magari essendo sempre, come la NATO intende fare e come la NATO afferma, in grado di mantenere quel "edge", quel vantaggio tecnologico, nei confronti degli avversari. Non so se ho risposto alla sua domanda.

Carlo Nordio:

Mi faccia capire.

È in tema di responsabilità. È possibile che un›intelligenza artificiale, auto clonazione, creando – cioè un programma che magari non era stato previsto da chi ha inserito gli algoritmi iniziali – entri in un sistema altrui, captando e magari alterando dati sensibili? E se questo accadesse, di chi sarebbe la responsabilità?

Visto che il cervello, l'intelligenza artificiale, non è responsabile penalmente, magari lo sarebbe civilmente. Però la captazione di dati sensibili, o addirittura l'alterazione, sarebbe un gravissimo rischio. È certamente un reato se commesso da una persona umana. Ma in questo caso c'è la possibilità che il creatore di questa intelligenza artificiale dica: "No, mi è scappato di mano, io non volevo, ha fatto tutto da solo."

Massimiliano Signoretti:

Sicuramente la capacità c'è. La capacità c'è. Questo fa parte dei programmi di addestramento e dei Safety Institute del Regno Unito.

Anche questo vale per le domande che vengono fatte ai sistemi di intelligenza artificiale per addestrarli a determinate risposte, ma questa è la parte difficile. Include anche addestrarli a quali sono le risposte indesiderabili. Quindi, questo fa parte di quel meccanismo di programmazione. È evidente che un sistema che è in grado di autodeterminarsi autonomamente, se viene meno quell›elemento fondamentale che è comunque il controllo umano sul processo – anche se «out of the loop» – ma comunque di mantenere un controllo, questo è possibile.

L'abbiamo visto con una propagazione, una proliferazione non controllata di codici malevoli. Questo avviene. Da un punto di vista del diritto, ferme restando le difficoltà di raccolta di evidenze digitali, che poi fanno chiaramente risalire all'autore, chi progetta o impiega in ultimo la capacità ha la responsabilità degli effetti, anche indesiderati, prodotti dall'impiego di quella capacità.

Chiaramente, tenendo conto che l'elemento psicologico rileva in alcuni reati e non rileva in altri, dipenderà sempre dallo studio e dall'analisi della fattispecie. Se questa prevede un elemento psicologico, allora è un conto. Se invece vi è un'oggettività nel danno, allora avrà un diverso valore.

Giovanni Salvi:

Posso aggiungere solo una cosa alla risposta del Colonnello Signoretti, molto netta. Sì, è possibile trasformare il contenuto di informazioni che si trova all'interno di un apparato. È possibile già da tempo ed è possibile anche con apparati molto semplici, con iniezioni di malware. Questo è un problema molto serio.

Le ultime modifiche normative prevedono la possibilità, nelle operazioni sotto copertura, non solo dell'apprensione dell'oggetto informatico che si attacca, ma anche la sua manipolazione. Questa questione sorse già nel 2016, quando io ero Procuratore Generale presso la Corte d'Appello di Roma e, quindi, avevo il ruolo di Giuseppe Amato. Noi allora concordammo con gli apparati di intelligence che l'utilizzo del malware e dei trojan fosse, per ciò che riguardava l'autorizzazione, limitato al solo ascolto e non comprendesse le attività di apprensione.

Questo è un tema estremamente importante, perché dal punto di vista giudiziario implica la necessità di certezza del dato acquisito, che potrebbe essere manipolato. Allo stesso tempo, però, è un fortissimo strumento: per esempio, potrebbe essere modificata una corrispondenza in un'organizzazione terroristica al fine di far cadere in trappola o farla saltare.

Il problema è enorme, e sono contento che sia emerso, perché spero che sia una delle cose di cui parleremo nei prossimi giorni.

Stefano Lucchini:

Grazie anche per le domande.

Grazie, Colonnello Signoretti. Complimenti, veramente molto chiaro, preciso, puntuale. Il tema è assolutamente affascinante. È quello anche della democrazia, a tutti gli effetti, sia da fattori esogeni – che sono i più pericolosi – sia, altrettanto, da quelli endogeni.

ATTUAZIONE DELLA GIURISDIZIONE PENALE NELLO SPAZIO VIRTUALE

Paola Severino

Presidente della Luiss School of Law e Professore Emerito di Diritto penale presso l'Università Luiss Guido Carli - già Ministro della Giustizia - Comitato scientifico FVO

Buongiorno a tutti,

saluto tutte le autorità presenti e, in particolare, il Ministro della Giustizia Nordio, con il quale condivido questo panel, nonché tutti gli autorevoli relatori.

Permettetemi altresì di rivolgere un sincero ringraziamento alla Fondazione Occorsio e, in particolare, al Procuratore Salvi, che, con un impegno e una passione davvero straordinari, si è fatto carico dell'organizzazione di questo importante incontro collaterale al G7, che vede riuniti eminenti esponenti delle istituzioni, di organizzazioni internazionali e del mondo accademico a discutere di un tema davvero centrale e pressante nello scenario attuale.

L'attuazione della giurisdizione nello spazio virtuale rappresenta invero una questione complessa che, ormai, da diversi anni tiene impegnati legislatori e operatori del diritto a livello globale e che peraltro, alla luce dell'incessante sviluppo delle nuove tecnologie – e, segnatamente, dell'Intelligenza Artificiale – richiede ulteriori, puntuali riflessioni. Con particolare riguardo al tema che mi è stato affidato – ovverosia quello dell'applicazione della giurisdizione penale – è noto come le caratteristiche tipiche del cyberspace – quali, ad esempio, la transnazionalità, l'aterritorialità e l'anonimato – rendano assai complicato individuare lo Stato – o gli Stati – nella cui giurisdizione ricade l'illecito. Se, infatti, sotto il profilo delle attività astratte, di delimitazione della giurisdizione, gli ordinamenti nazionali non trovano limiti significativi nel diritto internazionale, problemi ben più rilevanti si pongono a fronte dell'attivazione di una pluralità di iniziative punitive statali.

Il codice penale italiano, all'art. 6 – analogamente a quanto previsto in molti altri ordinamenti giuridici – si ispira, come noto, al criterio di universalità, nel definire quando un reato possa ritenersi commesso nel territorio dello Stato. Peraltro, è consolidato nella giurisprudenza di legittimità l'orientamento che ritiene sufficiente a fondare la giurisdizione italiana la commissione nel territorio dello Stato anche solo di un frammento della condotta, intesa in

senso naturalistico, e, quindi, di «un qualsiasi atto dell'iter criminoso, seppur privo dei requisiti di idoneità e di inequivocità richiesti per il tentativo», purché non si tratti di un proposito generico, privo di concretezza e specificità[8]

La tendenza degli ordinamenti nazionali, inoltre, a estendere la giurisdizione anche a fatti commessi al di fuori del territorio dello Stato è incentivata dalle previsioni di alcune Convenzioni internazionali, anche in materia di cybercrime. Basti pensare a quanto previsto dall'art. 22 della Convenzione di Budapest del 2001. Anche la nuova Convenzione delle Nazioni Unite sulla criminalità informatica – in procinto di essere adottata dall'Assemblea generale – consente agli Stati parti di fondare, in misura ancora più significativa, la giurisdizione su fatti commessi al di fuori del loro territorio, ad esempio se perpetrati in danno degli Stati stessi, o dei loro cittadini, o in presenza di determinate ipotesi di connessione, purché non vengano compiuti, all'estero, atti tali da mettere in discussione la giurisdizione di altri Paesi (artt. 22 e 5 della Convenzione). Inoltre, esiste la concreta possibilità che i reati informatici si configurino come reati transnazionali, qualora rispondano ai requisiti previsti dalla Convenzione di Palermo del 2006 e dalla legge n. 146 del 2006. In particolare, è sempre più incisivo il collegamento tra l'attività di gruppi criminali organizzati, anche operanti in più di uno Stato, e il cybercrime, come è emerso anche recentemente dalle indagini svolte sui cd. criptofonini, e sulle quali si sono pronunciate, nell'ultimo anno, le Sezioni unite della Cassazione.

Proprio in materia di reato transnazionale, l'art. 15 della Convenzione di Palermo costituisce un ulteriore fondamento normativo per l'estensione della giurisdizione degli Stati parti a reati commessi al di fuori del territorio degli Stati stessi. Simili previsioni, unitamente alle illustrate difficoltà relative all'individuazione del locus commissi delicti, rendono non remota l'eventualità dell'apertura di procedimenti penali paralleli, da cui possono derivare effetti fortemente negativi sotto i profili dell'esercizio del diritto di difesa, dell'assunzione delle prove, della tutela delle persone offese, della piena osservanza delle garanzie del giusto processo. Il rimedio estremo risultante quindi, eccessivamente tardivo e non idoneo a scongiurare questi effetti pregiudizievoli. Infatti, già diversi anni fa le Sezioni unite penali hanno valorizzato la nozione di litispendenza, che prescinde dall'intervenuta formazione di un giudicato, accogliendo un'interpretazione estensiva dell'art. 649 c.p.p.,

---

8 *Ex multis*, Cass., Sez. VI, 27 marzo 2024, n. 13063; Cass., Sez. VI, 21 settembre 2017, n. 56953, P.M. c. G.; Cass., Sez.
III, 2 marzo 2017, n. 35165; Cass., Sez. VI, 24 aprile 2012, n. 16115; Cass., Sez. VI, 7 gennaio 2008, n. 1180, L.

inteso quale «espressione di un principio più ampio, che, anche in assenza di una sentenza irrevocabile, rende la duplicazione dello stesso processo incompatibile con le strutture fondanti dell'ordinamento processuale[9]». Tuttavia, sono ancora poco efficaci gli strumenti volti a prevenire e a risolvere i conflitti di giurisdizione tra Stati. In materia cybercrime e di reati transnazionali, rispettivamente gli artt. ٢٢ della Convenzione di Budapest e ١٥ della Convenzione di Palermo individuano meccanismi di consultazione, nell'ipotesi in cui più Stati parti intendano esercitare la propria giurisdizione sui reati oggetto degli stessi trattati, o abbiano già avviato procedimenti. Anche la nuova Convenzione ONU in materia di cybercrime conferma tale tipologia di approccio (art. ٢٢). Si tratta, tuttavia, di previsioni poco pregnanti, che – non individuando modalità e possibili esiti del contatto tra i diversi Paesi coinvolti – rischiano di non riuscire a scongiurare gli effetti dell'apertura di procedimenti paralleli. Analoghe criticità possono essere riferite, nel più ristretto ambito dell'Unione europea, alla procedura di composizione dei conflitti di giurisdizione delineata dalla decisione quadro 2009/948, in ragione della natura non vincolante del meccanismo dalla stessa disciplinato e dell'assenza di una determinazione specifica e puntuale delle possibili soluzioni a cui esso può consentire di pervenire. Si tratta, in definitiva, di una normativa che pone in capo ai Paesi interessati, con l'intervento di Eurojust, determinati obblighi "procedurali", ma non quello di pervenire a un risultato: in caso di mancato accordo, infatti, potrà operare il rimedio ultimo del divieto di bis in idem.

Il problema dell'individuazione dello Stato più idoneo a perseguire il reato, e l'esigenza di evitare procedimenti paralleli, sono alla base anche della recente proposta di regolamento dell'Unione europea in materia di trasferimento dei procedimenti penali, del 2023. La proposta si inserisce negli obiettivi fissati nella strategia dell'UE 2021- 2025 per la lotta al crimine organizzato e sembra indubbiamente utile, considerando anche che la Convenzione del Consiglio d'Europa sul trasferimento dei procedimenti penali del 1972 è stata ratificata solo da tredici Stati, e che l'Accordo fra gli Stati membri delle Comunità europee sul trasferimento dei procedimenti penali del 1990 non è mai entrato in vigore, forse per la scarsa attrattiva di uno strumento idoneo a porre limitazioni all'esercizio della giurisdizione. Nello sviluppo dei negoziati, si è rilevata anche l'importanza di coniugare l'efficacia della repressione di illeciti che in misura crescente eccedono i confini nazionali con la salvaguardia dei diritti fondamentali, quali il diritto a un ricorso giurisdizionale effettivo e il rispetto delle prerogative della difesa.

---

9 2 Cass., Sez. Un., 28 giugno 2005, Donati.

Il trasferimento dei procedimenti penali, con riferimento ai reati ivi contemplati, è previsto altresì dalla nuova Convenzione ONU sul cybercrime (art. 39): la norma è destinata a costituire la base giuridica del trasferimento stesso, quando non siano in vigore altri trattati tra gli Stati parti che regolino tale profilo.

Proprio a fronte delle incertezze che riguardano la determinazione della giurisdizione, è essenziale che le autorità dei singoli Stati cooperino efficacemente nella prevenzione e nel contrasto della criminalità informatica. Un esempio virtuoso in questo senso è quanto previsto dalle direttive NIS (direttiva 2016/1148) e poi NIS2 (direttiva 2022/2255). Faccio riferimento, in particolare, all'istituzione del gruppo di collaborazione, della rete "CSIRT" dei punti di intervento e, da ultimo, del network EU CyCLONe (*European Cyber Crisis Liaison Organisation Network*). Se il gruppo di collaborazione può svolgere un ruolo significativo sotto i profili dello scambio di informazioni e di buone prassi, della condivisione di strategie di intervento, della valutazione congiunta dei rischi, tra i compiti della rete "CSIRT" si colloca proprio l'attuazione di una risposta coordinata a un incidente cyber rientrante nella giurisdizione di uno Stato membro, o a carattere transfrontaliero. Anche CyCLONe può fornire un supporto all'individuazione e gestione delle misure per fronteggiare simili eventi. Essenziale, in questi ambiti, è quindi l'attività delle Agenzie: in primo luogo l'Agenzia europea per la cybersicurezza – il cui ruolo operativo è stato rafforzato dal Cybersecurity Act (regolamento 2019/881) – e, nel nostro Paese, l'Agenzia per la cybersicurezza nazionale, istituita nel 2021.

L'importanza di un intervento coordinato delle autorità statali nella gestione di incidenti e minacce cibernetiche si coglie anche nella proposta di *Cyber Solidarity Act* dell'Unione europea, presentata nel 2023, che contempla l'introduzione di appositi meccanismi di gestione delle emergenze e di revisione degli incidenti, specialmente al fine di fronteggiare illeciti di rilevante impatto e su larga scala.

Vorrei, infine, solo fare cenno alla recente approvazione di rilevanti atti normativi sovranazionali, che costituiscono una risposta all'incerta definizione dei confini della giurisdizione statale in materia di cybercrime e all'esigenza di acquisire le prove elettroniche oltre i confini nazionali. Mi riferisco, nell'ambito eurounitario, al regolamento (2023/1543) e alla direttiva (2023/1544) che, dopo cinque anni dalla presentazione delle relative proposte da parte della Commissione, hanno introdotto gli strumenti dell'ordine europeo di produzione e dell'ordine europeo di conservazione delle prove elettroniche. Si tratta una dimensione innovativa del mutuo riconoscimento, fondata sul contatto diretto tra l'autorità giudiziaria di uno Stato membro e il presta-

tore di servizi, detentore dei dati, stabilito in altro Stato membro. Queste misure mirano a rendere più efficace l'accertamento dei reati, sebbene non manchino profili di criticità, come la variabilità dei presupposti che possono giustificare il provvedimento nei diversi ordinamenti, e la prevedibile difficoltà, per il prestatore di servizi destinatario dell'ordine, di vagliarne la legittimità.

Un approccio analogo caratterizza, inoltre, il secondo protocollo addizionale alla Convenzione di Budapest sulla criminalità informatica, che contempla, anch'esso, una procedura di cooperazione diretta con il service provider stabilito in altro Stato parte della Convenzione per l'acquisizione di diverse tipologie di dati. È significativa la firma del protocollo anche ad opera di Stati che non sono membri del Consiglio d'Europa; alcune previsioni in materia sono state inserite anche nella nuova Convenzione ONU, a cui ho già fatto riferimento (artt. 42 e 43).

L'auspicio è che le difficoltà nella delimitazione della giurisdizione statale, in relazione al cybercrime, non comporti un'inutile e pregiudizievole moltiplicazione di iniziative punitive – frutto della scarsa propensione a rinunciare a una fondamentale espressione della sovranità – ma sia invece il punto di partenza per lo sviluppo di un coordinamento efficace delle attività di prevenzione e repressione, a partire dall'Unione europea. Solo proseguendo su questa via, a mio avviso, sarà possibile fronteggiare le sfide, spesso imprevedibili, che la criminalità informatica continuerà a porre, anche nella sua dimensione transfrontaliera a queste sfide noi dobbiamo contrapporre la collaborazione tra Stati, perché la sfida verrà vinta, la battaglia verrà vinta, la guerra verrà vinta soltanto se gli Stati collaboreranno tra di loro e non si contenderanno, in chiave di fraintesa sovranità, la partenza di procedimenti penali che, duplicando le iniziative, le renderebbero meno efficaci.

Vi ringrazio.

PRIMA SESSIONE

GIURISDIZIONE, RESILIENZA E DIFESA ATTIVA QUALE EFFICACIA NELLO SPAZIO VIRTUALE?

GIURISDIZIONE, RESILIENZA E DIFESA ATTIVA QUALE EFFICACIA NELLO SPAZIO VIRTUALE?

PRESIEDE

Alessandro Pansa

Già Direttore del Dis e Capo della Polizia – Special Advisor AI FVO

Come abbiamo ascoltato dalle relazioni di questa mattina il tema della sicurezza nello Spazio Virtuale preoccupa i Governi di tutti i Paesi e l'attenzione che si pone, nei Fori internazionali, all'argomento ne sottolinea l'importanza.

Non vi è dubbio che l'IA sta già cambiando le nostre vite e lo farà in maniera più profonda nel futuro. Viviamo oggi una realtà diversa, viviamo anche la cosiddetta realtà virtuale. È questo uno spazio nuovo in cui dovremo vivere e convivere, per cui abbiamo bisogno di regole. Lo Spazio Virtuale ha bisogno del suo ordinamento giuridico. E la Giurisdizione è la base principale per definire il sistema delle regole. Questa esigenza, che direi del tutto logica e chiara, si scontra però con la complessità della realtà che bene ci è stata presentata nei vari interventi che hanno aperto i lavori del convegno.

Non li ripeterò, né mi dilungherò nell'approfondire le sfide che l'IA ci pone e le minacce che essa può rappresentare. Voglio solo sottolineare l'importanza della regolamentazione. Nei giorni scorsi ho partecipato, a Venezia, al XIV Trans-Regional Seapower Symposium, sul tema "A spotlight on the dephts: the Underwater as the new frontier for humankind". Vi erano i vertici delle Marine Militari di 69 Paesi, i rappresentanti di tutti gli organismi internazionali che si occupano del mare, esponenti del mondo accademico e dell'industria interessata al settore. Tutti hanno sottolineato che l'Underwater domain è una realtà nuova, che va dalla superficie del mare sino ai fondali e al sottosuolo marino, sconosciuta per l'80% per cento, che attira gli interessi di tutti perché offre opportunità di sviluppo (basti pensare che il sottosuolo marino contiene la stragrande maggioranza delle terre rare e delle risorse minerarie della Terra). Anche l'Underwater, come lo Spazio Virtuale, ha bisogno di regole, altrimenti i più forti e i più spregiudicati se ne approprieranno a danno di tutti gli altri. Tra potenze nazionali e multinazionali non ci saranno più di 10 soggetti che la faranno da padroni.

Lo Spazio Virtuale presenta lo stesso problema; prima verrà creata una cornice normativa e prima sarà possibile frequentarlo liberamente. Se non ci

saranno regole - sottolineo regole condivise – soggetti forti, sia a livello statuale che privato, se ne impossesseranno e lasceranno ai margini gli attori meno forti. Sono certo che il prosieguo dei lavori odierni ci consentirà di capire come affrontare questa sfida. Da ultimo consentitemi di portare alla vostra attenzione un mio dubbio.

Sono abbastanza fiducioso che si riuscirà a risolvere sul piano convenzionale il tema della giurisdizione e anche quello delle forme migliori di cooperazione giudiziaria internazionale. Certo non sarà facile: ma l'intelligenza dei giuristi coniugata con le capacità diplomatiche porteranno di sicuro a tracciare un perimetro entro il quale il giudice potrà esercitare la giurisdizione. La domanda che mi pongo a questo punto: saremo in grado tecnicamente di eseguire le azioni concrete che servono sia sul piano investigativo che dibattimentale all'acquisizione della prova?

La normativa internazionale, come quella che l'U.E. ha proposto la primavera scorsa, stabilirà ad esempio quali saranno le cose che non potranno essere fatte da alcuni, come l'acquisizione delle informazioni personali da parte delle aziende, ma consentite ad altri, ad esempio in sede di indagini preliminari.

Rimanendo all'esempio della privacy, il tema fondamentale da sciogliere sarà: chi detiene le informazioni? chi detiene la tecnologia per gestire questi dati? chi sarà in grado di proteggerli? saranno le diverse autorità giudiziarie in grado di implementare le loro attività con le tecnologie adeguate, necessarie per far giustizia?

È importante che noi tutti ci ricordiamo che non possiamo porci semplicemente la domanda su quali principi e quali regole disciplineranno la giurisdizione o l'acquisizione della prova. Dobbiamo porci anche la domanda: che cosa saremo in grado di fare per dare seguito alle norme che verranno emanate? Avremo la tecnologia che ci consentirà di assicurare l'applicazione corretta delle regole fissate? Avremo la tecnologia adeguata per garantire l'acquisizione della prova?

Noi siamo un Paese che non produce autonomamente microchip, non produce hardware complessi, insomma nel settore delle tecnologie dipendiamo essenzialmente nell'approvvigionamento dall'estero (un po' come per le fonti energetiche). Questo ci pone tecnicamente su un piano di debolezza. Va aggiunto che accanto alla carenza industriale, vi è anche quella rappresentata dalla circostanza che i grandi operatori del settore, le cosiddette OTT (over the top), sono tutti stranieri, principalmente statunitense e cinesi, ma non solo. Dobbiamo esser consapevoli che se – ad esempio - l'autore del reato fosse un OTT che risiede all'estero, qualora i trattati internazionali ci dessero la possibilità di processare una di queste compagnie in Italia, con quali strumenti ci

presenteremo nella sede di quell'azienda o meglio nelle sue sedi per acquisire la prova? avremo gli strumenti per entrare nei loro sistemi, per scandagliare le loro base dati? riusciremo ad accedere agli applicativi indispensabili per comprendere come hanno commesso il reato e avremo le tecnologie per acquisire la prova forense?

Credo che abbiamo una risposta: l'IA è il problema, ma anche la soluzione, in quanto non esiste una IA malvagia o criminale, ma esistono persone malvagie e criminali che la potranno usare. Per cui sono convinto che, consapevoli che non ci sarà mai un livello di sicurezza assoluta, dovranno essere individuati e adottati collettivamente i limiti comportamentali e le regole da applicare che lo Spazio Virtuale.

PRESENTAZIONE DEL MINISTRO DELL'INTERNO

Matteo Piantedosi
Ministro dell'Interno

Grazie ad Alessandro Pansa per aver introdotto gli importanti temi di questo dibattito, che è di grandissima attualità e interesse. Io parto da una considerazione: appena qualche giorno fa, l'Accademia reale delle Scienze svedese ha conferito il Nobel per la fisica a Geoffrey Hinton, i cui studi hanno aperto la strada alla moderna intelligenza artificiale.

La cosa che mi ha colpito è che il neo Premio Nobel, in numerose dichiarazioni pubbliche che hanno fatto seguito a questo riconoscimento, abbia voluto lanciare un forte monito sui rischi derivanti da un utilizzo malevolo di questa nuova tecnologia. E questo perché, come credo sia stato diffusamente già detto anche nell'introduzione di Alessandro Pansa, l'avvento dell'intelligenza artificiale sta segnando probabilmente l'inizio di una nuova era, piena di entusiasmanti opportunità.

Io sono molto d'accordo con quanto diceva: per opportunità, per il nostro benessere, ma anche per una serie di minacce. Quindi, è una grande opportunità, ma anche un tema rispetto al quale mettere in campo molte cautele. Minacce per le nostre società, che si stanno presentando ad un ritmo sconosciuto in passato.

Avverto il dovere connesso all'adempimento delle responsabilità istituzionali che derivano dal mio incarico, di sfruttare appieno tutte le potenzialità che questa tecnologia può garantire nel rafforzare la sicurezza, ma con la possibilità di proteggere l'esercizio dei diritti individuali e sociali. Proprio su questo paradigma, quindi sul paradigma dell'opportunità, ma nello stesso tempo dell'esigenza di tutela, durante il meeting dei ministri dell'Interno del G7 che si è tenuto la scorsa settimana, ho avuto modo di promuovere un dibattito sulle migliori strategie per rendere l'ecosistema digitale più sicuro e per garantire anche un uso etico dell'intelligenza artificiale. Devo dire che con i colleghi dei paesi membri di quel formato del G7 abbiamo discusso concretamente sulle principali minacce al nostro sistema di valori democratici, prendendo atto e constatando come queste minacce si esprimano in modo lesivo nel mondo reale e in quello digitale.

Il tema delle preoccupazioni legate all'affermazione dell'intelligenza artificiale non riguarda solo il mondo virtuale, ma anche i riflessi che ha nel

mondo concreto. Un primo tema di confronto è stato sicuramente tutto quello che riguarda i rischi per le nostre società derivanti da scenari di crisi internazionali. Ovviamente, quelle che più ci interessano in questi periodi sono i teatri di guerra dell'Ucraina e del Medio Oriente. È stato messo in luce come ci sia un'aggressiva ed incessante propaganda di matrice jihadista diffusa nel web, e che questa rappresenti una delle maggiori cause di radicalizzazione di soggetti responsabili di attentati sul suolo europeo. E quindi credo che già questo dia l'idea di come, dal virtuale, si possa poi tutto trasferire nel mondo reale, nel mondo concreto.

Inoltre, nell'occasione, abbiamo riservato attenzione sugli strumenti di contrasto alle interferenze malevole, un tema noto, quindi, alla disinformazione. Su questo abbiamo assunto precisi impegni, anche nella dichiarazione finale, per proteggere le nostre democrazie, soprattutto durante questa delicata fase delle competizioni elettorali. Questo perché si è convenuto sul fatto che non possiamo assistere passivamente ad azioni spregiudicate di attori malevoli che, avvalendosi dell'uso sempre più aggressivo di, ad esempio, deep fake, tentano di minare gli elementi di coesione sociale delle società liberali, indebolendo la fiducia dei cittadini nelle istituzioni democratiche e nei mezzi di informazione.

Uno degli elementi di maggiore novità che, come presidenza italiana, abbiamo voluto porre nell'agenda del G7 riguarda le nuove frontiere delle investigazioni finanziarie per contrastare l'uso illecito delle criptovalute, su cui credo che il nostro Paese vanti un'esperienza all'avanguardia.

È nato su questo specifico tema un fruttuoso scambio di idee che mi ha dato molta soddisfazione, sia con tutti i ministri del G٧, ma specialmente con la collega americana, la vice Attorney General Lisa Monaco, che era presente alla riunione. Abbiamo preso atto della difficoltà di assicurare alla giustizia i singoli autori dei reati che si schermano dietro l›anonimato del web e che sono protetti da giurisdizioni non sempre collaborative. Abbiamo convenuto, come ministri dell›Interno, che la via maestra non possa non essere quella di agire sempre in via preventiva, cioè con un attento monitoraggio nel web e, successivamente, attraverso la confisca dei proventi illegali.

Questo tema dell'azione preventiva è ricorso molto in tutti i temi che abbiamo posto in agenda, parlando del problema della cybersicurezza in generale e dei problemi variamente articolati legati alla diffusione e ai rischi dell'intelligenza artificiale. Si è parlato molto, nelle dichiarazioni finali, anche dell'intelligenza artificiale, e che questa fase avanzata di difesa debba passare assolutamente attraverso il coinvolgimento dei soggetti privati: gli internet provider, i grandi player che sono presenti nel mondo della produzione e diffusione di prodotti digitali, e quindi che deve esserci una grande alle-

anza tra le istituzioni pubbliche e le istituzioni private, che in qualche modo sono presenti sugli scenari globali.

È una strategia che intendiamo potenziare anche per la prevenzione e il contrasto della diffusione delle droghe sintetiche, in particolare il fentanil, il cui commercio avviene sempre più spesso nel dark web. Questo, sempre per dare un senso a come i temi legati alla cybersicurezza non si esauriscono all›interno del mondo digitale, ma hanno ripercussioni su fenomeni che incidono nel mondo reale, anche in termini tradizionali. E solo su questo campo abbiamo convenuto anche sull›esperienza americana, dove il tema della diffusione delle droghe sintetiche è molto più attuale. In Europa al momento è una preoccupazione forte, ma in America è già molto, molto impegnativo. Si è convenuto che solo indagini mirate di tipo telematico potranno consentire di interrompere la filiera dello spaccio e di procedere al sequestro degli enormi profitti illeciti che ne conseguono per i trafficanti.

Su questo importante tema, dirò che, sempre per rimanere un po' alle questioni di sicurezza nazionale che in qualche modo attengono alle funzioni e alla missione istituzionale di Ministro dell'Interno, sebbene possa apparire un ambito in qualche modo lontano dalla dimensione digitale, noi crediamo che dobbiamo puntare a una efficace azione di monitoraggio del web, anche per smantellare i cartelli dei trafficanti di migranti, attraverso azioni di oscuramento dei siti e delle pagine social che sponsorizzano le traversate del Mediterraneo. Un'attività che noi in Italia stiamo già facendo con le nostre istituzioni di polizia. Questo perché non possiamo accettare che le organizzazioni criminali propongano i loro servizi come dei qualunque tour operator, mettendo a repentaglio peraltro le vite delle persone e violando la prerogativa degli Stati di governare le politiche migratorie. Il contrasto al fenomeno del digital smuggling è uno dei pilastri su cui si poggia l'action plan contro i trafficanti che abbiamo approvato.

Il documento adottato al termine dei lavori sul mandato dei leader del G7, sul mandato che ci è derivato dai leader a Borgo Ignazia, declina le principali linee di azione che intendiamo portare avanti. Con i colleghi ministri degli Interni, in quell'occasione abbiamo convenuto su un principio di fondo: per vincere la sfida di rendere più sicuro il mondo digitale, dobbiamo stare un passo avanti rispetto ai criminali dal punto di vista tecnologico. Anche questo ritrovo in pillole nella presentazione che ha fatto Alessandro Pansa. A questo scopo le autorità di law enforcement devono avere il pieno dominio dei mezzi informatici per prevenire la commissione dei crimini e quindi avere la possibilità di individuare gli autori. Ed è proprio il tema delle potenzialità offerte dalle nuove tecnologie che è stato al centro della cena di lavoro che abbiamo dedicato all'intelligenza artificiale, impreziosita dai contributi dei guest speaker di livello internazionale.

C'è stato un contributo molto importante della vicepresidente di OpenAI, Anna Maccanio, che ha illustrato le incredibili prospettive di crescita delle capacità di calcolo dei sistemi di intelligenza artificiale. È stato evidenziato come, entro pochi anni, potremo contare su software in grado di svolgere autonomamente complesse operazioni che ci consentiranno di prevedere in modo sempre più accurato accadimenti futuri e i trend di fenomeni rilevanti in tutti i campi del sapere. C'è stato poi il contributo del direttore generale della Commissione europea, Roberto Viola, che ha messo in luce i principi ispiratori del nuovo regolamento europeo sull'intelligenza artificiale. Lo ha fatto nella visione dei contenuti essenziali di questo regolamento, che si rivolgono soprattutto alla doverosità di un utilizzo etico e responsabile dell'intelligenza artificiale. Questo perché, secondo la normativa europea appena adottata, la tecnologia non potrà mai essere utilizzata per manipolare le persone o per attribuire immorali punteggi di gradimento sociale ai cittadini, né per incidere sui diritti essenziali dell'individuo, come la libertà e la manifestazione del pensiero.

Quindi, una regolamentazione che, attraverso questi punti cardinali e quello più in generale della tutela della privacy e dei diritti fondamentali dei cittadini, ha già dato un orientamento su quello che deve essere il quadro dei limiti che devono caratterizzare la potenzialità dell'utilizzo dell'intelligenza artificiale. E proprio la centralità dei diritti dell'individuo è uno degli aspetti che io personalmente ho inteso evidenziare in tutte le occasioni in cui ho affrontato il tema. Questo perché, per evitare pericolose derivate applicative, credo che dobbiamo far sì che l'intelligenza artificiale non si sostituisca mai al nostro giudizio.

Il paradigma, questo, al di là degli sviluppi tecnologici, dovrà essere sempre questo: non immaginare mai che una tecnologia, qualsiasi sia lo sviluppo, possa sostituirsi agli elementi umani, agli elementi del giudizio, ma che possa fungere solo da supporto al giudizio umano. Gli operatori che utilizzeranno la tecnologia, sia nel campo medico che in quello del law enforcement, dovranno essere adeguatamente formati, non solo sulla capacità scientifica di interpretare le opportunità tecniche e tecnologiche, ma anche per interpretare e utilizzare i dati degli algoritmi in modo assolutamente responsabile, evitando di fare affidamento cieco sugli strumenti che gli vengono messi a disposizione e sovvertendo, quindi, ove necessario, l'esito della procedura informatica.

Avviandomi a conclusione, credo che questo G7 ci abbia dato la possibilità di avviare un dibattito proficuo sulle potenzialità che l'intelligenza artificiale può garantire nel rafforzamento della sicurezza e anche nella promozione dei diritti individuali e sociali. Sono molteplici i campi di applicazione

che abbiamo immaginato per un concreto utilizzo delle infinite capacità di elaborazione che questa nuova tecnologia può assicurarci.

Mi riferisco, per esempio, alla possibilità di dominare in tempo reale l'enorme mole di dati inseriti dalle forze di polizia, sia a livello nazionale che a livello mondiale, per non lasciare zone d'ombra in cui i criminali possano nascondersi. Oppure, si è parlato della cosiddetta "polizia predittiva", che grazie a un'analisi approfondita dei fattori di rischio può consentire di allocare le risorse delle istituzioni di polizia in modo più efficiente, consentendo interventi più efficaci, tempestivi e mirati. Questo, ovviamente, con l'obiettivo e l'unico scopo di proteggere i cittadini e ridurre il tasso di criminalità. Perché, come ho detto, l'intelligenza artificiale potrà essere estremamente utile anche per avere una panoramica più accurata sulle dinamiche e sulle cause dei flussi migratori, e disporre, per esempio, dei dati provenienti dai Paesi maggiormente coinvolti dal fenomeno dei flussi migratori e dai fenomeni correlati. Questo ci permetterebbe di avere prospettive di medio e lungo termine e di mettere in campo efficaci strumenti di prevenzione e di contrasto dei flussi stessi.

Peraltro, questi sono temi sui quali anche il nostro Presidente del Consiglio dei Ministri, anzi, soprattutto il nostro Presidente del Consiglio dei Ministri, ha avuto modo di intervenire durante l'assemblea generale delle Nazioni Unite a New York, occasione nella quale la Premier Meloni ha evidenziato come la comunità internazionale debba cooperare per impedire che questo dominio diventi una zona franca senza regole e come, per converso, sia necessario predisporre meccanismi di governance globale che siano capaci di assicurare il rispetto delle barriere etiche.

L'INTELLIGENCE IN UN MONDO CHE CAMBIA. IL DIFFICILE EQUILIBRIO TRA RESILIENZA E REAZIONE

Lorenzo Guerini
Presidente COPASIR

Nell'*Annual Progress Report* presentato a luglio di quest'anno dall'Open-Ended Working Group sulla sicurezza e sull'uso delle tecnologie di informazione e comunicazione (ICT) delle Nazioni Unite si legge che i Paesi partecipanti hanno rilevato un preoccupante aumento dell'uso malevolo, da parte di alcuni Stati, di campagne di informazione segrete basate sulle ICT per influenzare i processi, i sistemi e la stabilità generale di altri Paesi. Tali condotte minano la fiducia, possono innescare processi di *escalation* e possono minacciare altresì la pace e la sicurezza internazionale, nonché arrecare danni diretti e indiretti alle persone.

Nella relazione per il 2023 dell'Agenzia per la cibersicurezza nazionale, si sottolinea come le attività operative dell'Agenzia, sia nella fase preventiva di monitoraggio, analisi delle minacce e allertamento dei soggetti esposti ai rischi, sia nella fase reattiva di risposta agli incidenti, abbiano subito nel periodo di riferimento un notevole incremento in termini numerici rispetto all'anno precedente, «indice di un generale aumento delle attività cyber, rilevato anche a livello europeo e globale». In particolare, si evidenzia come dai dati emerga chiaramente un sensibile aumento delle segnalazioni indirizzate all'Agenzia e come, a fronte di un numero di comunicazioni ricevute sostanzialmente allineato a quello del 2022, siano aumentati di circa il 30% il numero di eventi cyber e più che raddoppiati gli incidenti. Immagino, ma il direttore Frattasi potrà confermarlo, che il trend per il 2024 non possa che confermare l'incremento dell'attività cui quotidianamente è chiamata l'Agenzia da lui diretta.

A ciò si aggiunge un aumento considerevole delle tensioni geopolitiche a livello mondiale che rendono particolarmente delicata la questione della cibersicurezza. Lo sviluppo delle nuove tecnologie e l'uso sempre più pervasivo di internet per tutte le azioni legate anche ai più banali gesti della vita quotidiana, nonché i crescenti impieghi dell'intelligenza artificiale, hanno determinato e continueranno senz'altro a determinare un radicale cambiamento nel concepimento stesso delle minacce da parte di attori, statuali e non, intenzionati a perpetrare azioni in danno di Paesi democratici come il nostro e persino delle stesse minacce con finalità di terrorismo. Pensiamo semplice-

mente ai danni che può arrecare un attacco informatico alla rete di un sistema ospedaliero, bloccando l'erogazione delle prestazioni sanitarie o potenzialmente anche assumendo il controllo di strumentazioni, il cui utilizzo è sempre più frequente, di telemedicina o di medicina robotica di precisione. Astrattamente sarebbe oggi più semplice eseguire un attentato aereo o ferroviario attraverso la violazione dei sistemi informatici piuttosto che con il posizionamento fisico di ordigni esplosivi o l'impiego di agenti dirottatori. O ancora si pensi al panico che potrebbe ingenerare la violazione di un sistema bancario, paralizzando le azioni quotidiane di milioni se non miliardi di cittadini.

Potremmo dire che la cibersicurezza poggia su due gambe altrettanto fondamentali: la prima è quella della resilienza delle nostre infrastrutture informatiche, su cui l'ACN sta svolgendo un lavoro estremamente importante fin dalla sua costituzione, che, anche al di là della risposta ai crescenti eventi che si verificano quotidianamente, poggia su una strategia che prevede anche un grosso sforzo di formazione di privati ed imprese ad un uso responsabile e attento delle tecnologie digitali. L'altra gamba è quella delle azioni di reazione e di prevenzione proattiva cui sono chiamati i nostri servizi di *intelligence* e il cui perimetro è stato disegnato con precisi paletti dal legislatore. Dalle semplici considerazioni che ho appena svolto discendono riflessi diretti sulle modalità attraverso le quali i nostri servizi di *intelligence* si trovano a reagire o a prevenire minacce in continua evoluzione e per loro stessa natura di difficile localizzazione *a priori*.

La gestione di tali operazioni, la cui adozione spesso deve avvenire in tempi estremamente rapidi per garantirne l'efficacia, pone, infatti, evidenti problemi sotto diversi profili, dall'autorizzazione preventiva al controllo successivo fino alle questioni più attinenti ai profili giurisdizionali ad iniziare dalla stessa competenza territoriale. A questo proposito, basti pensare come in ambito cibernetico nulla possa essere considerato scontato quanto ad attribuzione. Per risalire al soggetto che ha posto in essere un'azione o una minaccia, occorre, infatti, ripercorrere tutta la catena delle innumerevoli azioni di macchine automatizzate, risiedenti materialmente in spazi di territorialità diversi e spesso molto distanti non solo fisicamente ma anche dal punto di vista del quadro regolatorio. Qui vengono in gioco delicate questioni attinenti alla sovranità e alla differenza tra gli ordinamenti, coinvolgendo spesso la competenza anche di Stati terzi rispetto a quello del soggetto (o dello Stato stesso) che ha perpetrato l'attacco e a quello di chi l'ha subito, per il semplice fatto di avere ospitato nei rispettivi territori un pezzo di questa catena virtuale. Spesso le azioni necessarie per prevenire o rispondere ad un attacco presuppongono l'adozione di condotte che nel Paese ove risiedono i server, o anche in Italia, sono o possono essere considerate reato.

A tali questioni e in particolare a quelle più strettamente di carattere *intelligence* ha cercato di porre rimedio il legislatore con il decreto-legge 9 agosto 2022, n. 115, convertito, con modificazioni, dalla legge 21 settembre 2022, n. 142, recante appunto disposizioni in materia di *intelligence* in ambito cibernetico.

Il legislatore del 2022, peraltro in uno scenario di pieno conflitto in Ucraina, stabilisce con riferimento all'adozione «di misure di *intelligence* di contrasto in ambito cibernetico, in situazioni di crisi o di emergenza a fronte di minacce che coinvolgono aspetti di sicurezza nazionale e non siano fronteggiabili solo con azioni di resilienza, anche in attuazione di obblighi assunti a livello internazionale» un sostanziale parallelismo con lo schema, già collaudato nella legge n. 124 del 2007, relativo alle cosiddette garanzie funzionali. Come autorevolmente affermato dal dott. Salvi, il presupposto fondamentale di questa attribuzione di poteri è che gli attacchi rilevino sotto il profilo della sicurezza nazionale. In particolare, i valori tutelati sono quelli che si riconducono allo Stato comunità e che danno vita alla repubblica democratica, nella sintesi dell'ordine costituzionale, con particolari riferimenti ai profili della integrità del territorio e della sovranità, interna ed esterna, dello Stato. Questa precisazione è importante perché circoscrive fortemente il campo delle condotte che, previa autorizzazione dell'autorità competente, possono godere di particolari garanzie scriminanti proprio per la tutela di interessi vitali dello Stato.

La disposizione peraltro compie un importante salto di qualità nel prefigurare l'adozione di misure di contrasto, che ai sensi dell'articolo 7-*bis* del decreto-legge n. 174 del 2015, potevano essere intraprese «in situazioni di crisi o di emergenza all'estero che coinvolgano aspetti di sicurezza nazionale o per la protezione di cittadini italiani all'estero, con la cooperazione di forze speciali della Difesa con i conseguenti assetti di supporto della Difesa stessa».

L'articolo 7-*ter* del decreto-legge n. 174 del 2015, introdotto nel 2022, con riferimento alle azioni di contrasto in ambito cibernetico fa cadere ogni riferimento geografico e copre quindi anche eventuali azioni di contrasto poste in essere nel territorio della Repubblica.

Proprio in considerazione dell'ampiezza e della delicatezza dei poteri conferiti dalla norma, la medesima prevede che tutto l'impianto sia regolato da un provvedimento del Presidente del Consiglio adottato previo parere del COPASIR, volto a disciplinare il procedimento autorizzatorio, le caratteristiche e i contenuti generali delle misure che possono essere autorizzate in rapporto al rischio per gli interessi nazionali coinvolti, secondo criteri di necessità e proporzionalità.

L'esercizio di tali azioni di contrasto presuppone quindi, da un lato, un rigoroso vaglio autorizzatorio preventivo per le condotte scriminate, e dall'altro un esplicito richiamo alle garanzie funzionali come delineate dall'articolo 17 della legge n. 124 del 2007 che prevede espressamente dei limiti anche piuttosto stringenti all'utilizzo delle scriminanti medesime, come ad esempio la loro esclusione nei casi in cui la condotta prevista dalla legge come reato configuri delitti diretti a mettere in pericolo o a ledere la vita, l'integrità fisica, la personalità individuale, la libertà personale, la libertà morale, la salute o l'incolumità di una o più persone.

D'altro canto, il procedimento delineato, riportando tali azioni nell'ambito delle garanzie funzionali, comporta anche un controllo successivo del Comitato parlamentare per la sicurezza della Repubblica, cui devono essere trasmesse dal Presidente del Consiglio le comunicazioni relative allo svolgimento delle operazioni autorizzate sulla base della normativa richiamata. Il Comitato, a fronte di tali comunicazioni, pur senza entrare nella dinamica di operazioni in corso, è sempre nella facoltà di svolgere tutti gli approfondimenti che ritenga necessari, attraverso richieste documentali o richieste di audizione dei vertici dei servizi di *intelligence*. Ritengo che, soprattutto in tale ambito, il controllo successivo che il Comitato è chiamato ad esercitare possa risultare particolarmente importante e significativo.

In un contesto infatti in continua evoluzione, sia sotto il profilo degli strumenti utilizzabili, sia sotto il profilo della pervasività potenziale dell'azione dei servizi di *intelligence* negli spazi di libertà personale, nonché sotto il profilo della necessità di reazioni se non istantanee, almeno molto rapide, l'esistenza di un'istanza democratica cui dovere dare conto del proprio operato sia essenziale nel bilanciamento degli interessi in gioco.

A questo proposito, si potrebbe aprire un ampio ragionamento sulla asimmetria tra i vari attori, statuali e non, provenienti da sistemi diversi dal nostro e a noi potenzialmente ostili, che non soggiacciono alle stesse regole democratiche proprie del nostro Stato di diritto cui sono fortunatamente obbligati gli apparati dei Paesi democratici. Pensiamo anche alla enorme quantità di dati personali in possesso di potenze come la Cina e alle profonde differenze (per usare un eufemismo) di regolamentazione nella loro protezione, oppure alle massicce attività di disinformazione messe in campo da attori come la Russia. Nel nostro ordinamento si impone, da un lato, che le azioni di contrasto siano effettuate solo al ricorrere di effettive e concrete esigenze di sicurezza nazionale e, dall'altro, che le stesse rispettino comunque un criterio di proporzionalità.

Desidero infine accennare ad un'altra questione delicata che si pone con riferimento al reclutamento sia dei soggetti che sono chiamati a collaborare con le attività relative alla resilienza delle infrastrutture digitali, sia, a

maggior ragione, di quelli chiamati a svolgere sul campo le misure di *intelligence* di contrasto in ambito cibernetico.

Nel settore informatico, più ancora che nei settori di *intelligence* tradizionali, i profili tecnici di soggetti, in definitiva chiamati a svolgere un ruolo analogo a quello dei cosiddetti *hacker*, risultano estremamente appetibili sul mercato delle grandi società tecnologiche e la loro mobilità risulta decisamente elevata, a non volere considerare naturalmente l'ipotesi che possano essere reclutati da soggetti pubblici o privati appartenenti a Paesi, che in questa fase storica si pongono in modo antagonista. A tal proposito, occorre mettere in campo azioni che preservino l'investimento di formazione e il *know how* acquisito e tutelino anche i nostri apparati dalla possibile traslazione di conoscenze delicate. Non mi dilungo invece sui profili più attinenti alla giurisdizione perché sono sicuro che essi verranno affrontati con estrema competenza dagli altri relatori, a partire dal dott. Salvi che ha una grande esperienza in materia.

Desidero tuttavia associarmi all'invito che egli stesso ha formulato in altra sede ad adeguare gli strumenti sostanziali e processuali alle nuove dimensioni dei reati commessi nello spazio virtuale, al fine di evitare il proliferare di conflitti di attribuzione tra poteri dello Stato, allorché l'esigenza di accertamento si scontrerà con quella della prevenzione. Come abbiamo visto, nell'ambito cibernetico la dimensione spaziale e quindi l'individuazione della competenza territoriale appare estremamente labile. Gli stessi effetti delle misure adottate possono essere di difficile se non impossibile valutazione a priori. Pertanto, l'unica soluzione appare quella di un quadro regolatorio il più possibile chiaro nel delineare i paletti che lo Stato impone per potere consentire l'attivazione delle scriminanti, da abbinare ad un vaglio rigoroso ex ante da parte dell'autorità politica (Presidente del Consiglio e Autorità delegata), responsabile verso il Parlamento della propria condotta, nonché ad uno scrupoloso esame successivo del COPASIR.

La prassi applicativa che si formerà nei prossimi mesi e nei prossimi anni su tali disposizioni consentirà poi anche di aprire una riflessione sull'adeguatezza di un sistema che è chiamato a trovare un non facile equilibrio tra l'esigenza di fornire risposte immediate ed efficaci rispetto a minacce complesse e di spesso difficile individuazione e la salvaguardia di quei valori e principi anche di carattere costituzionale che regolano l'esercizio di funzioni così delicate dei nostri apparati di sicurezza.

Su questo il Comitato che mi onoro di presiedere farà la sua parte senza sconti, ma sempre in un'ottica di collaborazione istituzionale, svolgendo, anche attraverso l'utilizzo dello strumento delle relazioni al Parlamento previste dalla legge una funzione di stimolo, oltre a quella diretta di controllo.

IL CYBER COME STRUMENTO DEL TERRORISMO INTERNAZIONALE. NUOVE MINACCE – NUOVE RISPOSTE. IL PROBLEMA DELL'ATTRIBUZIONE. SPECIFICITÀ DELL'ATTRIBUZIONE NEL CYBERSPAZIO

Alessandra Guidi
Vice Direttrice DIS

L'intelligenza artificiale, e, in particolare, quella generativa, pur essendo una manifestazione relativamente recente di una tecnologia esistente da decenni, si inserisce in uno scenario eterogeneo e complesso, sollevando questioni fondamentali riguardo ai concetti di sovranità, giurisdizione e territorialità. La sua introduzione ha il potenziale di destabilizzare ulteriormente i paradigmi esistenti, rendendo ancora più urgente l'esigenza di un ripensamento giuridico e politico. Queste tecnologie emergenti stanno infatti modificando profondamente il contesto normativo e politico globale, sfidando l'efficacia degli strumenti normativi tradizionali e richiedendo un approccio interdisciplinare per affrontare le loro implicazioni socioeconomiche e geopolitiche. L'intelligenza artificiale rappresenta, dunque, un elemento chiave nel plasmare il futuro equilibrio geopolitico, favorendo le nazioni che saranno in grado di governarla con efficienza e lungimiranza. Non sorprende, pertanto, che le principali potenze globali, come Stati Uniti, Cina, Arabia Saudita e diverse altre nazioni, stiano investendo ingenti risorse nello sviluppo e nell'applicazione dell'IA. La dimensione degli investimenti in questo campo non riguarda solo la costruzione di capacità tecnologiche, ma anche la creazione di un ecosistema integrato, che supporti l'innovazione e il controllo di questa tecnologia strategica.

L'intelligenza artificiale, di per sé, non è una tecnologia radicalmente innovativa: il suo potenziale risiede nella straordinaria quantità di dati oggi disponibili e nella crescente capacità computazionale. La disponibilità di questi due fattori si sta espandendo a ritmi vertiginosi, sollevando la questione di chi effettivamente detenga la proprietà dei dati e, di conseguenza, il controllo di fatto degli algoritmi che su questi ultimi vengono "addestrati". Tali dati, spesso, non appartengono a singoli Stati, organizzazioni o società, introducendo così importanti implicazioni di carattere geopolitico, economico e sociale. La capacità di raccogliere e utilizzare questi strumenti determina infatti un significativo vantaggio competitivo a livello internazionale, aumentando il divario tra i Paesi che dispongono delle risorse (dati e potenza computaziona-

le *in primis*, ma anche talenti) per sfruttare tali tecnologie e quelli che, invece, non possedendole, ne sono esclusi.

L'IA si fonda, dunque, su due "pilastri": la disponibilità dei c.d. "*big data*" e una capacità computazionale avanzata, fattori che, come abbiamo detto, stanno rapidamente assumendo una rilevanza centrale nel panorama globale. Basti pensare che, nel 2024, il numero di utenti di Internet ha raggiunto quasi i 5,5 miliardi, corrispondenti a circa due terzi della popolazione mondiale. Inoltre, il numero di dispositivi connessi ha superato gli 8 miliardi, contribuendo a generare un volume di dati fondamentale per l'addestramento dei modelli di IA. La proliferazione dei dispositivi connessi e la loro crescente capacità di interagire tra loro senza intervento umano stanno creando un ecosistema digitale altamente complesso, in cui la quantità e la qualità dei dati disponibili sono destinate a crescere esponenzialmente.

Un simile scenario pone sfide significative alla sicurezza nazionale e internazionale. La capacità dell'intelligenza artificiale di elaborare enormi quantità di dati in tempi brevissimi la rende una straordinaria opportunità, ma anche un potenziale vettore o "facilitatore" di minacce molto serie. Un esempio eclatante è quello dei c.d. *deep fake*: la capacità di generare contenuti video falsi, ma altamente realistici, ha già dimostrato la sua pericolosità: oltre alle sempre più insidiose e verosimili truffe, pensiamo ai potenziali impatti politici, economici o sulla pubblica sicurezza che potrebbero derivare dalla diffusione, ad esempio, di false dichiarazioni da parte una figura politica o di governo, arrivando a mettere a rischio la stabilità politica e la fiducia nelle istituzioni.

Anche minacce apparentemente più ordinarie, come il *phishing*, stanno diventando sempre più sofisticate grazie all'uso malevolo dell'IA, divenendo quasi indistinguibili da comunicazioni lecite e reali. Questi attacchi non solo sono in grado di ingannare individui comuni, ma anche di colpire le organizzazioni più strutturate, con conseguenze potenzialmente devastanti. Inoltre, algoritmi avanzati possono essere impiegati per analizzare codici alla ricerca di vulnerabilità nei sistemi informatici, automatizzando la ricerca dei bersagli. I *malware* dotati di capacità di "auto-addestramento" rappresentano un ulteriore pericolo: una volta introdotti in un sistema, sono in grado di migliorare continuamente le proprie strategie di evasione e infiltrazione. Tali considerazioni divengono ancor più attuali e rilevanti quando ci si rivolge ad infrastrutture critiche o sensibili, come quelle sanitarie: un attacco ai danni anche di una singola azienda sanitaria locale – da cui dipendono diverse strutture, ospedali e presidi sanitari –, infatti, può avere impatti notevoli, con effetti a cascata che vanno ben oltre il singolo soggetto colpito.

Un ulteriore aspetto che non va trascurato è che l'IA stessa, in quanto algoritmo, è attaccabile. Lo si può fare in vari modi: "avvelenando", ad esem-

pio, i dati stessi su cui questa viene addestrata. Questo fenomeno è estremamente insidioso, poiché comporta il rischio (di per sé già intrinseco all'IA stessa, in quanto i suoi processi decisionali interni sono caratterizzati da "opacità") di introdurre risultati inattesi, fuorvianti o persino pericolosi, compromettendone irrimediabilmente l'affidabilità: se i dati che alimentano gli algoritmi sono alterati, anche le applicazioni che si basano su di essi saranno alterate, con conseguenze significative sugli *output* prodotti da queste tecnologie che, va ricordato, sono e saranno sempre più presenti e pervasive.

In tale contesto, il concetto di resilienza diventa cruciale: come la madre di Winnicott, noto psicoanalista e pediatra britannico del secolo scorso, la sicurezza perfetta "non esiste", esiste quella "sufficientemente buona". Anche con difese altamente sofisticate, esiste sempre la possibilità che una minaccia passi inosservata o che un attacco particolarmente elaborato riesca a superare le misure di protezione. L'importante, e qui entra in gioco la resilienza, è sviluppare la capacità di rialzarsi, riprendersi e reagire dopo il colpo subito, ripristinando l'operatività dei sistemi e assicurando la continuità dei servizi nel più breve tempo possibile, minimizzandone le conseguenze negative.

Si pensi, di nuovo, all'esempio del settore sanitario: un attacco andato a buon fine, in questi casi, potrebbe comportare l'interruzione di servizi essenziali e terapie salvavita, bloccando pronto soccorso, ambulanze e sale operatorie. Ed è un fenomeno che non riguarda soltanto l'Italia, ma tutti i Paesi più avanzati. Per questo motivo, è essenziale implementare misure che riducano al minimo i danni causati da un attacco e garantire il più rapido ripristino dei servizi.

In quest'ottica, l'Agenzia per la Cybersicurezza Nazionale (ACN) ha adottato il concetto di resilienza come principio guida, con l'obiettivo di garantire il ripristino tempestivo dei sistemi compromessi e proteggere, così, anche la sicurezza nazionale nello spazio cibernetico. Il che si traduce, concretamente, in pratiche operative che vanno dalla progettazione di sistemi più robusti alla formazione di personale specializzato, fino alla creazione di protocolli di risposta coordinata che coinvolgano sia il settore pubblico che quello privato.

La resilienza cibernetica ha recentemente ricevuto un importante riconoscimento giuridico attraverso la Legge n. 90/2024, che, oltre a disciplinare più diffusamente i rapporti operativi e i raccordi informativi tra ACN, Autorità Giudiziaria e Polizia Giudiziaria, ha introdotto opportuni meccanismi di bilanciamento tra le esigenze investigative e quelle di resilienza nazionale, funzionali ad assicurare l'efficace e tempestivo svolgimento delle attività di ripristino, l'assicurazione delle fonti di prova e il coordinamento del Procuratore Nazionale Antimafia e Antiterrorismo (PNAA).

In particolare, la norma ha previsto che l'Agenzia debba informare il PNAA della notizia di un attacco ai danni di determinati sistemi informatici o telematici e, in ogni caso, quando risulti interessato un soggetto Perimetro, NIS o Telco, e che il pubblico ministero informi l'ACN quando acquisisce notizia di alcuni gravi reati informatici, assicurando anche il raccordo informativo con il CNAIPIC. Inoltre, la medesima Legge ha introdotto specifici meccanismi di bilanciamento tra indagini e resilienza, prevedendo: da un lato, che il PM impartisca le disposizioni necessarie ad assicurare che gli accertamenti urgenti siano compiuti tenendo conto delle attività svolte dall'Agenzia a fini di resilienza; dall'altro, che, per evitare un grave pregiudizio per il corso delle indagini, il PM possa disporre il differimento delle attività di resilienza con provvedimento motivato.

Un caso emblematico è stato l'arresto di un giovane hacker, resosi responsabile di un attacco ai sistemi della Giustizia italiana: grazie alla collaborazione tra l'ACN, la DNA, le Procure inquirenti e la Polizia Postale, è stato possibile mettere in sicurezza i sistemi compromessi senza inficiare le indagini in corso, assicurando così la continuità dei servizi critici nel rispetto delle esigenze investigative. Questa esperienza ha dimostrato l'efficacia di un approccio coordinato e sinergico alla gestione degli incidenti di sicurezza – che sono anche reati, ma non solo –, evidenziando l'importanza della cooperazione tra le diverse istituzioni coinvolte.

Il dominio cyber è un dominio diverso dagli altri: è trasversale, sfaccettato e mutevole. È un dominio nel quale siamo immersi tutti in prima persona. Di conseguenza, bisogna riconoscere che la resilienza e la sicurezza cyber poggiano sulle spalle di ciascuno di noi: su ogni singola azienda, su ogni singola istituzione, su ogni singolo cittadino. Solo attraverso un approccio olistico, dunque, si riuscirà, se non ad eliminarlo, a ridurre il rischio cyber a un livello quantomeno "fisiologico".

Un tale approccio, per realizzarsi compiutamente, poggia su un elemento fondamentale: la cultura. Possiamo spendere milioni di euro per mettere in sicurezza i sistemi, ma se un dipendente non adotta tutte le cautele necessarie e, ad esempio, durante lo *smart working*, collega il computer di servizio alla rete domestica senza precauzioni ogni investimento rischia di rivelarsi futile. Per una mancanza di cultura della sicurezza, viene così vanificato lo sforzo complessivo di un'intera organizzazione. È, pertanto, fondamentale investire sulla formazione e sulla diffusione della consapevolezza dei rischi cyber a tutti i livelli e in tutti i settori, soprattutto con riguardo alle sfide e alle opportunità offerte dalle nuove tecnologie in un mondo sempre più digitalizzato.

In conclusione, tornando sul tema dell'intelligenza artificiale, emblematico dell'epoca che stiamo vivendo, vorrei chiudere ribadendo che l'IA

offre opportunità straordinarie, ma pone anche sfide enormi, in particolare per quanto riguarda la sicurezza nazionale nello spazio cibernetico, e non solo. In un simile scenario, caratterizzato dalla diffusione dell'IA quale potenziale strumento offensivo, difensivo e piattaforma di attacco, la resilienza si rivelerà un elemento ancor più cruciale per garantire la stabilità e la sicurezza del nostro Paese di fronte a minacce nuove, emergenti o semplicemente diverse.

Il futuro della sicurezza nazionale, ma anche quello della sicurezza di ciascuno di noi, dipenderà dalla nostra consapevolezza e capacità di integrare tecnologie avanzate, sviluppare strategie efficaci di difesa e resilienza, e garantire che le risposte agli attacchi siano coordinate e proporzionate alle minacce. In definitiva, la resilienza, abilitata dalla cultura, rappresenta non solo una strategia difensiva, ma anche una componente fondamentale della capacità di un Paese di prosperare in un ambiente sempre più digitalizzato e interconnesso.

ACN (AUTORITÀ NAZIONALE PER LA CYBERSICUREZZA) E LA SALVAGUARDIA DELLA SICUREZZA NAZIONALE NELLO SPAZIO VIRTUALE

Bruno Frattasi
Direttore dell'Agenzia per la Cybersicurezza Nazionale

Una breve, ma necessaria premessa.

Guardando agli ultimi sviluppi del dibattito speculativo sulla definizione della sicurezza nazionale, precisamente sui suoi contenuti e limiti, ha fortemente influito l'attuale e drammatico clima di belligeranza. Già da tempo vengono riportati alla sicurezza nazionale e fatti rientrare in essa, aspetti che riguardano la conservazione e la stabilità di determinati beni e interessi, soprattutto pubblici, secondo una visione eccessivamente allargata e, per questo, tale da snaturare l'essenza autentica del concetto. Non vi è dubbio, però, che, quale che sia la configurazione del concetto di sicurezza nazionale che assumiamo, venga ad occupare in esso un peso via via crescente la dimensione cibernetica, venuta ad aggiungersi alla dimensione politico-istituzionale, a quella economico-finanziaria e a quella energetica. Tutte, ciascuna e nel loro insieme, attengono e chiamano in causa la salvaguardia della comunità politica nazionale, con l'obiettivo comune di proteggere cittadini, istituzioni e imprese, da ogni tentativo di interferenza, ingerenza o pressione, interna o esterna, che possa anche solo compromettere la continuità della vita del Paese, scalfendone la libertà e l'autodeterminazione.

Negli stessi termini, con un accenno forte alle funzioni essenziali dello Stato, si esprime anche l'art. 1 della Legge che ha istituito cinque anni orsono il Perimetro di sicurezza nazionale cibernetica. Pare evidente, dunque, che la sicurezza nazionale sia compenetrata con il principio di sovranità, intesa nel senso classico di plenitudo potestatis; sicché la sicurezza nazionale, nello spazio virtuale, si presenta – intanto ed in primis – come un predicato della sovranità digitale nazionale. Senonché abbiamo a che fare, e già da qualche tempo, con un'altra forma di sovranità digitale, quella europea. Espressione "immaginifica e di grande forza evocativa" che risale al discorso tenuto dalla Presidente Von der Layen sullo stato dell'Unione nel 2020.

Come è stato notato, tale espressione - la sovranità digitale europea, contiene un'affermazione politica e non giuridica, indica un obiettivo cui tendere e non descrive uno stato di fatto già acquisito e consolidato. Soprattutto essa si iscrive in una logica di competizione e di confronto tra potenze globa-

li in cui la dimensione nazionale viene inevitabilmente trascesa, sovrastata, ma, come tenterò di chiarire, niente affatto obliterata o eclissata; sicché anche in questa sua forma, quella sovranazionale europea, la sovranità digitale rimane ancora legata alla sicurezza nazionale, pur acquisendo una ricchezza ed una forza ulteriori rispetto alla sola dimensione domestica, e non attingibili se non nel contesto unionale. Il mio intervento è rivolto a illustrare, anche con brevi esempi, come l'Agenzia si ponga a servizio della sicurezza nazionale, sia che questa rimanga funzionale alla affermazione della sovranità digitale nazionale, sia che si ponga nell'orizzonte della sovranità digitale europea.

Il contributo dell'Agenzia alla sicurezza nazionale ha un suo sicuro ancoraggio nella già citata legge istitutiva del Perimetro di sicurezza nazionale cibernetica. Come sappiamo, essa fu concepita ed è stata attuata per delimitare – in assenza di un chiaro indirizzo nella prima direttiva NIS – strutture e superfici informatiche (reti, sistemi e servizi) necessariamente da proteggere secondo i più elevati standard di sicurezza tecnologica, definiti (e qui la precisazione non è una trascurabile forma di acribia del legislatore) "a livello internazionale e dell'Unione Europea".

L'attività dell'Agenzia si esprime qui in alcuni sostanziali momenti: i) il primo, consiste nella partecipazione al processo di definizione, soggettiva e oggettiva del Perimetro; partecipazione che avviene assumendo un ruolo centrale che si declina anche in una funzione di coordinamento, secondo la trama che le stesse disposizioni della legge fondativa dell'Agenzia si sono incaricate di portare a evidenza successivamente alla introduzione del Perimetro, e avendo cura di stabilire gli opportuni raccordi tra i due corpi normativi. Per incidens, volendo scolpirne con maggiore incisività il ruolo coordinamentale, è qui il caso di ricordare quanto venne disposto dall'Agenzia all'indomani dello scoppio del conflitto russo-ucraino, allorché, in attuazione di una disposizione normativa urgente, emanata in quella temperie, dispose nei riguardi di tutte le amministrazioni pubbliche che nell'approvvigionamento dei dispositivi di protezione venisse seguito un criterio di necessaria diversificazione, atto a scongiurare forme di dipendenza tecnologica che avrebbero potuto esporre inopportunamente al rischio cyber la nostra superficie digitale e compromettere la stessa sicurezza nazionale; ii) un altro momento in cui trova espressione la peculiare funzione dell'Agenzia rispetto ai soggetti nonché ai beni e ai servizi inclusi nel Perimetro, riguarda l'attività del Centro di Valutazione e di Certificazione Nazionale, la quale attività si concreta, in casi di particolare complessità, nello scrutinio tecnologico di beni, sistemi e servizi ICT destinati ad essere impiegati in quella parte di superficie informatica inclusa nel Perimetro, con l'ulteriore conseguenza che la valutazione, preventivamente eseguita, sull'affidabilità dei nuovi asset deve tener conto anche del

contesto d'uso, cioè del loro ambito di impiego, come limpidamente chiarisce la norma. Possono scaturire dallo scrutinio condizioni e prescrizioni che poi vengono ad essere trasfuse nelle procedure di approvvigionamento delle entità appartenenti alla constituency del Perimetro e a formare oggetto di clausole vincolanti inserite nei bandi di gara affinché venga garantito il più assoluto rispetto delle indicazioni impartite dall'Agenzia; iii) la tutela del perimetro di sicurezza nazionale cibernetica si concreta anche nella fissazione di termini assai ristretti entro i quali i soggetti che vi sono inclusi hanno l'obbligo di comunicare all'Agenzia gli impatti subiti a carico della parte di superficie digitale oggetto di tale speciale protezione.

Ancora più che in altri ambiti, appare qui fondamentale l'immediatezza di reazione e di risposta all'incidente. Conseguentemente, l'interlocuzione da stabilire tra il soggetto colpito e il CSIRT-Italia – struttura interna all'Agenzia – non può che conformarsi a criteri e dettami operativi di estrema sollecitudine, in grado di assicurare rapidità e precisione di intervento. Sono perciò imprescindibili la preventiva e puntuale conoscenza, da parte dell'Agenzia, delle strutture digitali impattate nonché di coloro che ne hanno la piena responsabilità e che, per questo, sono chiamati a dialogare e a collaborare, a incidente avvenuto, con il CSIRT-Italia. Prima con una direttiva del Presidente del Consiglio dei Ministri del dicembre 2023, in seguito con una norma di legge che ne ha in parte replicato i contenuti immettendoli nell'ordinamento giuridico nazionale, si è particolarmente insistito sulla necessità – proprio a cominciare dalle Amministrazioni del Perimetro – di affinare e rafforzare gli aspetti collaborativi sollecitando gli attori pubblici a predisporre o ad aggiornare, ove esistenti, i piani di risposta e di gestione degli incidenti e, in caso di impatto, a prestare agli operatori dell'Agenzia la massima cooperazione perché il ripristino della piena funzionalità della parte digitale compromessa avvenga nel più breve tempo possibile. L'attività di sostegno e di supporto, insomma, è tanto più destinata al successo quanto più il soggetto, nei cui confronti tale attività si dispiega e viene prestata, si dispone ad accoglierla, conferendo ogni necessaria informazione sull'organizzazione di cybersecurity, anche con riguardo a terze parti coinvolte.

Ora, ma qui il discorso per ragione evidenti di brevità non può essere fatto che per larghi cenni, l'avvento della direttiva NIS2 - il decreto trasposito è recente ed entrerà in vigore il prossimo 16 ottobre - comporterà un gravoso impegno volto al rafforzamento della postura di cybersicurezza in molti settori, compresi quelli ora coperti dalla disciplina del Perimetro. Si tratterà di vedere se, proprio in ragione di questo ampio ombrello protettivo rappresentato dalla nuova disciplina NIS, non sia forse più che opportuno riconsiderare la configurazione e l'attuale estensione del Perimetro, affinché la

sicurezza nazionale digitale sia ancor meglio precisata e definita, venendo in tal modo a rappresentare pienamente quell'ideale "cassaforte" in cui riporre e custodire i "gioielli della corona". E questo anche al fine di stabilire la più conveniente reciprocità tra sistema- Perimetro e sistema-NIS, da considerare più su un piano di integrazione che non di pura e semplice alternatività.

Si è detto prima che la difesa della sovranità digitale passa dalla capacità di garantire la sicurezza nazionale impedendo forme di ingerenza che possano condurre alla perdita di controllo dei dati o della tecnologia di asset strategici. Da questo punto di vista, vale soffermarsi su due profili d'ingaggio dell'Agenzia che, seppure sotto angolature diverse, sono tuttavia entrambi dimostrativi dell'assunto accennato in premessa, circa la conciliabilità della sovranità digitale nazionale con quella europea; nel senso che non è che l'una debba cedere il passo all'altra, avendo smarrito, in qualche modo, il presupposto del suo esercizio, ma nel senso che la prima rappresenti il mattone, lo strato di sicurezza digitale su cui, appunto, la seconda possa ben fondarsi.

L'ascesa verso la dimensione sovranazionale non può e non deve corrispondere al "sacrificio" di quella nazionale, né alla sua obliterazione: Paesi europei più deboli e meno garanti della loro sicurezza nello spazio virtuale potrebbero solo concorrere a mantenere l'Europa in una condizione di maggiore fragilità e vulnerabilità, oltre a renderla meno presente e influente nel contesto globale. Prendiamo ad esempio, in questa direttrice, lo sforzo compiuto per sostenere la transizione al cloud delle Amministrazioni pubbliche centrali e territoriali, che ha visto l'Agenzia impegnata nella qualificazione del Polo Strategico Nazionale, la prima struttura cloud del Paese ad essere stata certificata al massimo livello di sicurezza, quindi, in grado di ospitare qualsivoglia tipo di dati, compresi quelli strategici, in quanto tali rilevanti per la sicurezza nazionale. Mi riferisco anche, rimanendo in questo ambito, all'approvazione recente dello schema nazionale di certificazione delle piattaforme cloud, che precorre la definizione e il varo dello schema europeo. Qui la costruzione di un modello normativo per il mercato digitale unionale che ne eviti la frantumazione interna si misura sì con l'esigenza di promuovere, nel gioco competitivo, l'autonomia tecnologica continentale, ma, altresì e soprattutto, con la necessità di assicurare il pieno controllo dei dati, senza distinzioni o eccezioni di sorta, presupposto perché si abbia una reale sovranità del patrimonio informativo nazionale, di ciascuna nazione.

L'obiettivo di un cloud sovrano europeo non potrà, una volta realizzato, che porsi a servizio, rafforzandola, della sicurezza nazionale dei vari Stati membri; il che conferma che non si sta parlando di istanze diverse e incomunicabili, bensì della stessa istanza, vista, da un lato, nell'interesse della sovranità del singolo Paese, dall'altro, nella prospettiva europea, pertanto, all'in-

terno della strategia di indipendenza tecnologica regionale più volte indicata.

Un ulteriore esempio, tra gli altri possibili, del contributo fornito dall'Agenzia alla difesa della sicurezza nazionale, possiamo trarlo dall'esercizio degli speciali poteri governativi connessi all'applicazione della normativa Golden Power, dopo che essa è venuta a includere tra le attività di rilevanza strategica i servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G, nonché "beni, rapporti, attività e tecnologie rilevanti ai fini della sicurezza cibernetica", nel cui novero è incluso anche il cloud. Per il vero, l'apporto dell'Agenzia alle attività del Gruppo di coordinamento che siede presso la Presidenza del Consiglio dei ministri con il compito di istruire le decisioni del Governo, ha riguardato anche ambiti diversi, stricto sensu, dalla cybersicurezza, e si è esteso, infatti, anche ad altri beni e rapporti ogni qualvolta fossero toccati aspetti legati sensibilmente al digitale, a conferma della natura abilitante della sicurezza informatica e della sua rilevanza trasversale. Per fornire una misura di tale apporto, nel 2023 l'Agenzia ha espresso il suo parere, contribuendo anche alla decisione di esercizio dei poteri di veto, in circa il 30 per cento delle notifiche presentate ai sensi della normativa Golden Power. Percentuale che è cresciuta nell'anno in corso, riguardando, allo stato attuale, quasi la metà delle notifiche.

In uno specifico caso trattato nel corso di quest'anno - un'operazione acquisitiva che interessava il settore finanziario-, l'Agenzia ha chiesto che tra le prescrizioni vincolanti figurasse anche quella relativa alla conservazione delle misure organizzative adottate dalla società target, incluso il mantenimento della localizzazione del patrimonio informativo sul territorio nazionale, o comunque europeo, a tutela della riservatezza, della sicurezza e del controllo dei dati, classificati come sensibili. L'estensione della disciplina sul controllo dell'acquisizione di asset strategici anche al settore cyber ha spostato il focus sull'approvvigionamento di beni e servizi in quanto risultino oggetto di determinati contratti e solo se le controparti contrattuali siano fornitori extraeuropei.

In questa scia, si pone anche la recente norma, contenuta nella legge 90 di quest'anno, secondo la quale, con un regolamento presidenziale di prossima adozione, andranno definiti i casi in cui per garantire la sicurezza nazionale dovranno essere privilegiate proposte o offerte che contemplino l'uso di tecnologie di cybersicurezza affidabili. Nel novero di quel trust la disposizione comprende, naturalmente, le tecnologie italiane, ma vi aggiunge quelle di Paesi appartenenti all'Unione Europea o aderenti alla Nato. Il provvedimento attuativo, inoltre, potrà individuare Paesi terzi con i quali intercorrano con le citate entità e organizzazioni sovranazionali accordi di collaborazione in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione.

La norma stabilisce che, con lo stesso decreto, vengano definiti gli elementi essenziali di cybersicurezza che le pubbliche amministrazioni tenute all'osservanza del CAD devono considerare ai fini dell'approvvigionamento di beni e servizi informatici allorché essi siano impiegati in un contesto d'uso afferente alla tutela di interessi nazionali strategici. È la stessa norma a chiarire che con la dizione di "elementi essenziali di cybersicurezza" sono da intendersi i criteri e le regole tecniche che nel loro insieme garantiscano, rispetto al rilievo degli interessi da proteggere, la confidenzialità, integrità e disponibilità dei dati da trattare. Viene ribadita, per questa via, l'istanza rivolta ad affermare nei settori cruciali per la vita e l'integrità del Paese il principio di indipendenza tecnologica e di sovranità del dato.

La minaccia cibernetica è globale ed incrementale, e lo è nel senso sia quantitativo che qualitativo. Gli attacchi dei criminali informatici alle infrastrutture critiche sono in costante aumento, specie nelle aree del mondo economicamente più ricche e dove l'espansione della superficie digitale esposta è più consistente. La minaccia più temuta è rappresentata dal ransomware, duplicemente insidiosa perché compromette gravemente la sicurezza dei dati, la cui esfiltrazione e crittazione è funzionale al ricatto estorsivo, e in misura notevole incrina anche la sicurezza economica. Per tali evidenti ragioni, il fenomeno del ransomware è stato oggetto, con la ricordata legge 90, di un intervento legislativo di rafforzamento della risposta punitiva che ha introdotto severi inasprimenti delle pene. Ma la diffusione mondiale della minaccia e il suo inasprirsi hanno portato alla costituzione di una vasta alleanza internazionale, la Counter Ransomware Iniziative, il cui obiettivo consiste nel definire un piano d'azione condiviso, capace di contrapporsi in maniera coesa al fenomeno senza che alcun punto di permeabilità o di inefficace resistenza possa favorire la catena criminale, e ciò appunto in virtù della sostanziale convergenza delle policy nazionali di contenimento e di risposta.

Questa iniziativa, che vede cooperare più di sessanta Paesi, è seguita con grande attenzione dall'Agenzia e rappresenta, accanto alla costante partecipazione ai Tavoli e ai gruppi di lavoro di Bruxelles, una parte significativa quanto rilevante della sua azione a livello internazionale. In questa come in altre forme di cooperazione multilaterale, sembra affacciarsi, anche sulla scena dello spazio virtuale, il principio di sicurezza collettiva, posto a mutua garanzia dell'integrità e dell'indipendenza dei Paesi che liberamente aderiscono ad un vincolo di alleanza.

Certamente il carattere incrementale della minaccia alla sicurezza nazionale è anche legato allo sviluppo delle tecnologie emergenti. Si stagliano, su questo sfondo, la tecnologia quantistica e l'intelligenza artificiale: la natura duale che le accomuna ci consente di dire, tuttavia, che lo sfruttamento

positivo di entrambe può alimentare e rafforzare, rendere più incisiva ed efficace la risposta alla minaccia. È questo il campo di impegno più prospettico a cui corrisponderà una modificazione strutturale e anche operativa dell'Agenzia, prefigurata dalla creazione, prevista dalla legge 90, del Centro nazionale di Crittografia e dall'impiego, all'interno del nostro Organismo, di personale militare anche funzionale al disimpegno, nell'ambito del Nucleo di sicurezza cibernetica, dei compiti discendenti in materia di cyberdefence dal Memorandum d'Intesa sottoscritto con la NATO. L'integrazione tra la componente civile e quella militare va perseguita e attuata convintamente, in considerazione della natura della minaccia e della sua offensività multidominio. Proprio per tale carattere, per la "fluidità" dei contesti in cui agisce e la sua a- territorialità, essa da sempre si connota come minaccia ibrida, con potenziali effetti di tipo sistemico.

In presenza di un siffatto scenario, sarebbe impossibile, ma soprattutto sbagliato, pensare in maniera non olistica alla sicurezza nazionale cibernetica, cioè in una maniera che non considerasse, con la dovuta attenzione, le esigenze della più stretta cooperazione tra tutte le strutture, comprese quelle dell'intelligence, deputate a tale forma di sicurezza del Paese. Ovviamente, ciascuna operante nel rispetto del proprio ruolo e secondo la propria missione.

STRUMENTI NORMATIVI INTERNAZIONALI. DAL MANUALE TALLINN 2 AL MANUALE TALLINN 3. FOCUS SUL RUOLO DELLA GIURISDIZIONE

Marko Milanovich
Professore di Diritto Internazionale Pubblico - Coordinatore Manuale Tallinn 3.0 - Centro di Eccellenza per la Difesa Cibernetica della NATO

Sono un professore di diritto internazionale e non un'autorità nel contesto italiano, quindi offrirò una prospettiva accademica sui temi legati alla giurisdizione e agli sviluppi della legislazione internazionale, con particolare riferimento alla cybercriminalità.

Il concetto di giurisdizione, nel diritto internazionale, si riferisce al potere di uno Stato, in quanto entità sovrana, di emanare e far rispettare le proprie leggi entro determinati limiti, senza violare la sovranità di altri Stati. Questo principio è centrale per comprendere come il diritto internazionale si adatti alle nuove realtà tecnologiche. Il Manuale di Tallinn è un progetto accademico, indipendente ma supportato dal Centro di Eccellenza per la Cyber Difesa della NATO. Esso tenta di adattare il diritto internazionale esistente, spesso vecchio di secoli, alle sfide poste dal cyberspazio. Poiché è molto difficile per gli Stati concordare nuovi trattati in materia, l'approccio è stato quello di reinterpretare le normative esistenti per affrontare le nuove sfide tecnologiche. Il primo manuale, pubblicato nel 2013, riguardava l'applicazione del diritto alla guerra cibernetica. Il secondo ampliava l'ambito a temi generali come la sovranità, l'intervento e i diritti umani nel contesto cyber. Attualmente, si sta lavorando a una terza iterazione, prevista per il 2027, che aggiornerà il manuale con le pratiche sviluppate negli anni intermedi.

La giurisdizione è solo una parte del Manuale di Tallinn. Esistono varie tipologie di giurisdizione, come quella prescrittiva (il potere di emanare leggi) e quella esecutiva (l'applicazione pratica delle leggi). Lo Stato può esercitare la propria giurisdizione su fatti avvenuti sul suo territorio o che coinvolgono cittadini o interessi nazionali, anche se tali fatti si verificano al di fuori del territorio. Ad esempio, un reato commesso contro un cittadino italiano all'estero può essere perseguito dalle autorità italiane. Nell'ambito cyber, il principio di territorialità è complesso. Un crimine come l'hacking può avvenire simultaneamente in più Stati: dove ha origine, dove viene completato e dove sono situate le infrastrutture informatiche coinvolte. Ciò rende possibile l'applicazione della giurisdizione da parte di più Paesi. Tuttavia, ci sono si-

tuazioni più sfumate, come il mero transito di dati attraverso Stati terzi, che sollevano interrogativi su quali giurisdizioni possano essere esercitate.

Un esempio recente è il rinvio a giudizio da parte degli Stati Uniti contro cinque membri dell'intelligence russa per l'uso del malware WhisperGate, progettato per colpire l'Ucraina. Sebbene gli Stati Uniti avessero un collegamento minimo con i crimini in questione, hanno giustificato la loro giurisdizione basandosi sul fatto che i sistemi informatici americani erano stati sondati dai responsabili.

La giurisdizione esecutiva, cioè l'applicazione delle leggi al di fuori del territorio nazionale, è ancora più problematica. Un'azione come l'interrogazione di un testimone tramite videoconferenza richiede spesso il consenso dello Stato in cui il testimone si trova. Allo stesso modo, accedere a dati ubicati in un altro Paese, ad esempio su un cloud, può essere difficile senza il consenso del Paese ospitante. La convenzione di Budapest e il suo protocollo addizionale cercano di affrontare tali situazioni, ma molte complessità rimangono irrisolte. La Convenzione delle Nazioni Unite sul Cybercrime ha rafforzato la cooperazione internazionale, ma non ha introdotto meccanismi per consentire a uno Stato di ordinare direttamente a un'azienda situata in un altro Stato di fornire dati. Questo riafferma il principio tradizionale di sovranità statale.

In conclusione, il diritto internazionale nel contesto cyber rimane radicato nei principi tradizionali di sovranità e consenso. Tuttavia, la prassi degli Stati continuerà a evolversi, affrontando le sfide poste dalla tecnologia.

LE DIVERSE CONFIGURAZIONI SULLA DEFINIZIONE E GLI ATTRIBUTI DELLO SPAZIO VIRTUALE. LE LORO CONSEGUENZE SULL'ESERCIZIO DEI POTERI SOVRANI E SULLA COOPERAZIONE GIUDIZIARIA

Dennis Wilder

Già alto funzionario dell'intelligence USA - Professore presso la School of Foreign Service della Georgetown University - Membro del National Committee sulle relazioni USA-Cina

Come probabilmente saprete, gli Stati Uniti sono sotto l'assedio di Cina, Russia e altri nel cyberspazio, e l'intelligenza artificiale è una componente importante di questi attacchi malevoli. Come ha spesso dichiarato Lisa Monaco, vice procuratore generale degli Stati Uniti, le 115.000 donne e uomini del Dipartimento di Giustizia degli Stati Uniti sono impegnati in una strategia informatica proattiva che dà priorità alle interruzioni a breve termine e alla protezione delle vittime, affrontando al contempo il più ampio ecosistema che sostiene i criminali informatici, compreso l'abuso di criptovalute e tecnologie dirompenti. Come ha dichiarato, gli Stati Uniti hanno un piano d'azione "incentrato sulla prevenzione, sulle interruzioni e sulle vittime".

Non illustrerò tutte le varie iniziative del Dipartimento di Giustizia, perché potete trovarle da soli. Permettetemi invece di parlare della pura e semplice audacia di alcuni attacchi da parte di Cina e Russia. Organizzazioni di hacking con sede in Cina, come Volt Typhoon, Flax Typhoon e Salt Typhoon, si sono infiltrate con successo nelle reti informatiche dei sistemi di infrastrutture critiche degli Stati Uniti e dei fornitori di servizi Internet (ISP) statunitensi. Secondo l'Office of the Director of National Intelligence's 2024 Annual Threat Assessment, questo tipo di infiltrazioni è destinato all'uso bellico da parte della Cina nei conflitti militari per danneggiare la capacità degli Stati Uniti di utilizzare le risorse fornite dalle loro infrastrutture critiche, il che rallenterebbe la formulazione di adeguate strategie militari statunitensi.[10]

- Secondo la Cyber Security and Infrastructure Security Agency (CISA), Volt Typhoon ha compromesso con successo le reti informatiche di strutture per le comunicazioni, l'energia, i trasporti, l'acqua

10 https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf

e le acque reflue negli Stati Uniti continentali e nei suoi territori, tra cui Guam;[11]

- Secondo un comunicato stampa del Dipartimento di Giustizia del 18 settembre, invece, il Federal Bureau of Investigation ha interrotto con successo una rete di bot organizzata da Flax Typhoon che conteneva 200.000 dispositivi e aveva compromesso con successo aziende, agenzie governative e fornitori di telecomunicazioni degli Stati Uniti.[12]
- Il 26 settembre, il Wall Street Journal ha riferito che Salt Typhoon si era introdotto nelle reti degli ISP statunitensi. Se gli hacker avessero avuto accesso ai router centrali degli ISP, sarebbero stati in grado di accedere a informazioni sensibili e ai dati personali dei cittadini americani.[13]

Secondo il CISA[14], gli obiettivi e le tecniche di infiltrazione di questi gruppi di hacker sono significativamente diversi dai modelli tradizionali di spionaggio informatico degli hacker cinesi. A differenza del tradizionale spionaggio informatico cinese, che ha preso di mira la proprietà intellettuale delle aziende utilizzando attacchi informatici rapidi, queste nuove operazioni informatiche privilegiano la non individuazione e la longevità per inserirsi con successo e rimanere dormienti all'interno dei server dei sistemi infrastrutturali per un periodo prolungato.

- Secondo Microsoft, Volt Typhoon utilizza una serie di contromisure per rendere difficile il rilevamento delle sue attività, tra cui l'utilizzo di credenziali legittime di individui registrati nella directory delle reti IT delle infrastrutture critiche.[15] Microsoft ha anche affermato che Flax Typhoon ha utilizzato tattiche simili per rimanere inosservato il più a lungo possibile.[16]
- Diverse fonti, tra cui Microsoft e CISA, hanno dichiarato che queste organizzazioni di hacker cinesi danno priorità alla longevità delle loro infiltrazioni e controllano frequentemente per assicurarsi di avere ancora accesso ai sistemi compromessi nel tempo. Questo permette loro di nascondersi nelle reti informatiche per anni in attesa di

11 https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a
12 https://www.justice.gov/opa/pr/court-authorized-operation-disrupts-worldwide-botnet-used-peoples-republic-china-state
13 https://www.wsj.com/politics/national-security/china-cyberattack-internet-providers-260bd835
14 https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a
15 https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/
16 https://www.microsoft.com/en-us/security/blog/2023/08/24/flax-typhoon-using-legitimate-software-to-quietly-access-taiwanese-organizations/

causare danni ai loro obiettivi.[17]

- Secondo il generale Timothy Haugh, direttore della National Security Agency, la presenza di hacker sostenuti dallo Stato cinese nelle reti informatiche delle infrastrutture critiche, che offrono poco valore per la raccolta di informazioni, è preoccupante perché suggerisce che la Cina sta posizionando risorse informatiche per colpire e interrompere le infrastrutture critiche nel caso in cui si verifichi un conflitto militare tra Stati Uniti e Cina.[18]

Utilizzare gli hacker per interrompere la capacità delle infrastrutture critiche di funzionare correttamente consentirebbe alle forze armate cinesi di ottenere un vantaggio iniziale in futuri conflitti militari con gli Stati Uniti. Se i cyberattacchi rendessero inutilizzabili infrastrutture critiche come i sistemi di comunicazione, prima di potersi concentrare sulla creazione di una strategia militare, gli Stati Uniti dovrebbero ripristinare questi sistemi per consentire il coordinamento tra le unità militari e le linee di rifornimento. Pertanto, è probabile che il governo cinese utilizzi gli hacker per attaccare le infrastrutture critiche degli Stati Uniti nelle prime fasi di un futuro conflitto militare tra i due Paesi.

- Inoltre, è molto probabile che alcuni gruppi di hacker sostenuti dalla Cina siano rimasti inosservati e continuino a minacciare la sicurezza e il funzionamento delle infrastrutture critiche degli Stati Uniti. Attacchi a sorpresa da parte di organizzazioni sconosciute inserite nelle reti delle infrastrutture critiche causerebbero danni significativi e sarebbero difficili da difendere per gli Stati Uniti.
- Se i gruppi di hacker cinesi prendono di mira le infrastrutture civili e militari, l'interruzione di risorse come l'acqua e l'elettricità non solo rallenterebbe le risposte efficaci dell'esercito statunitense durante un conflitto, ma danneggerebbe anche le popolazioni civili degli Stati Uniti. Se gli hacker cinesi riuscissero a mantenere interrotte le risorse essenziali per un periodo prolungato, probabilmente le sofferenze del popolo americano sarebbero amplificate.

Questo tipo di attacco informatico sfacciato ha molte implicazioni. La prima è che questi attacchi non fanno distinzione tra aziende statunitensi e straniere. Chiunque sia coinvolto nelle infrastrutture statunitensi è un bersaglio facile per gli hacker cinesi.

---

17 https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

18 https://www.wsj.com/politics/national-security/china-is-prepositioning-for-future-cyberattacksand-thenew-nsa-chief-is-worried-5ede04ef?mod=article_inline

La seconda implicazione è che, sebbene gli Stati Uniti possano essere il primo obiettivo, non saranno l'unico bersaglio di questo tipo di attacchi. Nel contesto dello stallo dello Stretto di Taiwan, Pechino non vorrà degradare solo le infrastrutture statunitensi, ma anche quelle degli alleati e dei partner statunitensi che intervengono in difesa di Taiwan. Possiamo quindi ipotizzare che Pechino stia già pianificando programmi simili non solo contro Taiwan, ma anche contro alleati degli Stati Uniti come il Giappone, le Filippine, l'Australia e il Regno Unito.

La terza implicazione è che è inevitabile che le azioni della Cina portino gli Stati Uniti e i loro più stretti alleati a esplorare lo sviluppo di proprie capacità offensive contro l'energia cinese e altre infrastrutture. Ciò che la Cina sta facendo porterà inevitabilmente a un'escalation della corsa agli armamenti cibernetici, in cui entrambe le parti cercheranno di posizionarsi per utilizzare lo spazio cibernetico come un regno di guerra che moltiplica le forze. Per quanto riguarda un altro elemento degli attacchi informatici assistiti dall'intelligenza artificiale, gli Stati Uniti stanno sperimentando il più alto livello di campagne di influenza malevola straniera nell'attuale ciclo di campagna presidenziale che abbiamo mai visto. Il 4 settembre, il Dipartimento di Giustizia ha annunciato che gli hacker russi sponsorizzati dallo Stato hanno dato a una società chiamata "Social Design Agency" 10 milioni di dollari per generare, utilizzando l'intelligenza artificiale, contenuti su Internet progettati per minare la fiducia del pubblico americano nel processo democratico. Gli agenti di Putin hanno anche utilizzato inconsapevoli influencer statunitensi per creare contenuti dannosi. L'interferenza dell'Iran è stata ancora più audace. Tre hacker iraniani hanno lanciato per diversi anni attacchi malevoli a funzionari governativi ed ex funzionari e giornalisti statunitensi. Di recente hanno inviato e-mail non richieste alla campagna di Biden contenenti informazioni non pubbliche rubate alla campagna di Trump per minare la corsa alla presidenza di Donald Trump. L'approccio della Cina alle campagne di influenza malevole è stato più sottile. Garphika ha identificato 15 account su "X" o Twitter che imitano cittadini statunitensi e gruppi di difesa che mettono in dubbio la legittimità delle elezioni americane. Uno di questi post ha avuto 1,5 milioni di visualizzazioni.

L'ultima domanda che vorrei pormi è: perché i cinesi e i russi sono così audaci?

Una paranoica estrema

Credo che il leader cinese Xi Jinping agisca spesso nel modo in cui agisce su questioni come il cyber maligno a causa dell'estrema paranoia degli Stati Uniti e dei suoi alleati.

- Xi ha spesso fatto riferimento alla "mano nera" della CIA nel fomentare i disordini a Hong Kong e ritiene che le rivoluzioni colorate siano opera dell'Occidente. Durante un colloquio privato con il Presidente Obama, ha affermato che la Cina è stata bersaglio di "rivoluzioni colorate", preannunciando la sua ossessione per la sicurezza nazionale.[19][20]
- La cosa più rivelatrice sono state le sue osservazioni a margine del Congresso Nazionale del Popolo nel marzo 2023, in cui ha dichiarato: "I Paesi occidentali, guidati dagli Stati Uniti, hanno attuato un contenimento e una repressione a tutto tondo della Cina, che ha portato sfide gravi e senza precedenti allo sviluppo del Paese".[21]

La paranoia di Xi si estende anche ai suoi amici di un tempo. Oggi l'ex vicepresidente Wang Qishan, che è stato determinante nella campagna anticorruzione di Xi, non può incontrare visitatori stranieri. Allo stesso modo, l'ex guru dell'economia Liu He, con cui Xi era amico fin dalle elementari, è scomparso e si dice che sia stato accusato di corruzione a causa delle attività commerciali del figlio. La paranoia di Xi è stata quasi certamente rafforzata dalla saga dell'ex ministro degli Esteri Qin Gang. Si ritiene che la giornalista di Hong Kong Fu Xiaotian, amante di Qin Gang, fosse una spia di una potenza occidentale. Qin Gang sembra aver convinto la leadership di essere stato semplicemente vittima di una trappola di miele e di non aver mai tradito Xi o la Cina. Qualunque sia la verità, Xi sembra aver deciso che sia nel suo interesse retrocedere Qin Gang a membro ordinario del partito. [22]

Con l'avanzare dell'età, è probabile che le sue tendenze paranoiche si accentuino. Sembra che Xi abbia deciso di non nominare un successore per poter rimanere leader della Cina a vita. Ha attaccato i leader di successo dell'industria tecnologica emergente cinese, come Jack Ma, perché li considera un potenziale centro di potere alternativo e una minaccia alla sua autorità.[23] La sua ossessione per la sicurezza nazionale lo ha portato a espandere notevolmente il potere del Ministero della Sicurezza di Stato, che è diventato sempre più audace nell'avvicinare gli uomini d'affari occidentali in Cina e nel metterli in guardia dalle attività anti-regime.

---

19 Remarks by President Obama and President Xi Jinping in Joint Press Conference | whitehouse.gov (archives.gov)

20 GT Investigates: US wages global color revolutions to topple govts for the sake of American control - Global Times

21 China accuses U.S. of containment and warns of potential conflict: NPR

22 Ex-Chinese FM Qin Gang loses seat at party top table but may escape punishment | South China Morning Post (scmp.com)

23 The vanishing billionaire: how Jack Ma fell foul of Xi Jinping (ft.com)

La Cina vuole un nuovo ordine mondiale

Un secondo aspetto del pensiero cinese sull'uso malevolo del cyber è che i cinesi vogliono rimodellare l'ordine internazionale in modo che rifletta i loro valori. Alla fine del 2017, Xi ha iniziato a parlare di "cambiamenti mai visti in 100 anni". L'implicazione era che gli Stati Uniti, come gli imperi britannico e francese degli anni Venti, erano in declino a lungo termine, mentre la Cina era sulla traiettoria per diventare la nazione più potente del mondo entro la metà del secolo. Al termine del suo incontro al vertice con il presidente Putin a Mosca nel marzo 2023, Xi Jinping è stato sentito dire: "In questo momento ci sono cambiamenti che non si vedevano da 100 anni e siamo noi a guidare questi cambiamenti insieme". Il presidente russo ha risposto: "Sono d'accordo".

La narrazione di un Occidente in declino e di un Oriente in ascesa può essere messa in discussione, soprattutto ora che la Cina sta lottando per recuperare lo slancio economico e la Russia è impantanata in una guerra apparentemente senza via d'uscita in Ucraina. Tuttavia, la narrazione del declino del potere degli Stati Uniti serve in ultima analisi allo scopo di Xi. Si adatta bene al suo "sogno cinese" di una grande potenza ringiovanita che domina gli affari mondiali entro il 2049, il centesimo anniversario della fondazione della Repubblica Popolare Cinese.

Il punto di partenza per comprendere la visione di Xi è la sua Iniziativa per la sicurezza globale. La GSI si fonda sull'avversione di Pechino per l'ordine internazionale guidato dagli Stati Uniti, riflettendo una competizione ideologica tra i due Paesi. Al 20° Congresso del Partito dello scorso anno, Xi Jinping ha differenziato in modo non troppo sottile la politica estera cinese da quella che definiva la politica estera degli Stati Uniti, dichiarando: "Abbiamo promosso in modo esaustivo la diplomazia dei grandi Paesi con caratteristiche cinesi... e ci siamo opposti senza riserve a qualsiasi unilateralismo, protezionismo e prepotenza. Abbiamo promosso la costruzione di un nuovo tipo di relazioni internazionali e partecipato attivamente alla riforma e alla costruzione del sistema di governance globale".

Le autorità cinesi considerano questo ordine occidentale come una concessione alla Cina di privilegi e di appartenenza al "club" privilegiato solo se la Cina si comporta secondo le norme e i valori occidentali. Ritengono che Washington usi il suo potere e le sue alleanze per limitare lo sviluppo della Cina, tra cui le sanzioni dell'amministrazione Biden nei confronti di oltre 300 aziende cinesi per violazione delle leggi statunitensi e le restrizioni sul trasferimento di tecnologie di intelligenza artificiale e quantistica alla Cina. Questo trattamento li convince che gli Stati Uniti non tratteranno mai la Cina come un pari, perché Washington è determinata a mantenere la Cina debole e a rimanere la potenza preminente del mondo.

Quindi, dal punto di vista di Xi Jinping, l'azione malevola contro gli Stati Uniti e l'Occidente nel cyberspazio è semplicemente un'estensione della lotta "senza esclusione di colpi" che ritiene di dover vincere per la sopravvivenza del comunismo cinese.

LE IMPLICAZIONI PER LE GIURISDIZIONI PENALI INTERNAZIONALI DELLE OPERAZIONI NELLO SPAZIO VIRTUALE

Rosario Aitala
Giudice - Primo Vice Presidente della Corte Penale Internazionale - L'Aia

Io mi sposterò su un terreno un po' diverso da quello che è stato affrontato finora, che è quello dell'ordinamento internazionale in senso proprio. L'ordinamento internazionale disciplina prevalentemente un mondo di Stati, ma nella materia di cui mi occupo quotidianamente ha anche dei riflessi sulle attività di individui, di soggetti.

Mi tocca un'avvertenza. Io parlerò di una serie di temi che astrattamente possono attagliarsi a diversi conflitti in corso in varie parti del mondo; naturalmente non mi riferisco a nessuno di questi, non potrei farlo perché io presiedo la sezione preliminare della Corte Penale Internazionale, quindi me ne occupo professionalmente e sono vincolato al segreto. Alcune operazioni svolte nello spazio virtuale in senso proprio oppure condotte attraverso strumenti elettronici, strumenti automatici, macchine e algoritmi, possono qualificarsi come crimini internazionali. Possono quindi comportare delle conseguenze nell'ordinamento internazionale in quanto tale. Le giurisdizioni internazionali, in particolare la Corte Penale Internazionale, ha giurisdizione su crimini internazionali che proteggono degli interessi molto elevati: la pace, la sicurezza internazionale, fondamentali in senso sistematico delle popolazioni del mondo, crimini di guerra, crimini contro l'umanità, genocidio e aggressione.

Presenterò tre o quattro macro-temi che però posso soltanto tracciare, indicando in qualche modo una mappa dei problemi che non posso naturalmente né affrontare né risolvere. Tolgo dal tavolo subito il primo, perché è stato in vari momenti affrontato anche dal Presidente Guerini, quello dell'utilizzazione di modalità cibernetiche per commettere attentati, atti di sabotaggio, attacchi a infrastrutture critiche. Questi atti possono qualificarsi come atti di terrorismo, come crimini di guerra, crimini contro l'umanità, in base alle diverse circostanze. È un tema apparentemente abbastanza ovvio, però non ci sono applicazioni giurisprudenziali, applicazioni pratiche; credo che il Presidente Guerini l'abbia coperto in modo assolutamente adeguato.

Il secondo tema che invece è più complesso ed è molto attuale è quello dell'uso, come metodo, come modalità di guerra, oppure come modalità di

controllo governativo delle popolazioni, di sistemi di apprendimento automatico, sistemi che normalmente vengono chiamati di Intelligenza Artificiale, ma sono in realtà dei sistemi di Machine Learning, cioè sono dei sistemi che lavorano attraverso degli algoritmi a cui viene insegnato cosa fare. Vengono indicati dei parametri e poi vengono offerti una serie di dati; questi sistemi li analizzano e li utilizzano a una velocità assolutamente inimmaginabile per qualsiasi essere umano.

Una prima applicazione, che non è recente, ormai è utilizzata da molti anni, è quella dei sistemi di armi automatiche. Sono delle armi che, una volta che vengono lanciate, hanno uno spazio di discrezione, per così dire; possono decidere in tempo reale cosa fare, identificare obiettivi, adattarsi all'ambiente circostante e lanciare attacchi a certi obiettivi senza nessun intervento umano. Decidono quindi autonomamente, una volta attivate. Il problema giuridico, ma anche etico, che comportano è che, se non sono adottate misure adeguate, il controllo umano cade, e mentre uno dei pilastri del diritto internazionale umanitario del diritto dei conflitti armati è il principio di precauzione, che obbliga gli Stati ad adottare delle accortezze in modo da non colpire soggetti estranei alle ostilità, civili o militari fuori combattimento e oggetti civili.

Questo tema è stato dibattuto già da un po' di tempo ed è stato risolto temporaneamente attraverso il criterio del *controllo umano significativo*, cioè si richiede che resti un controllo umano, che permetta di evitare che la macchina, soprattutto il drone, decida di colpire alcuni soggetti perché sembrano dei miliziani, ma non lo sono, oppure alcuni edifici che sembrano degli edifici di interesse militare ma non lo sono.

Da un punto di vista giurisdizionale, questo può comportare una serie di conseguenze rispetto a chi decide la politica dell'uso dello strumento, a chi lo manovra e a chi l'ha programmato. Secondo, ci sono dei sistemi detti DSS, in inglese *Decision Support System*, dei sistemi di assistenza alle decisioni della condotta delle operazioni belliche. Come funzionano? L'algoritmo accumula una serie di informazioni: sono informazioni di intelligence, dati telefonici, dati biografici, sesso, età, luogo di residenza, circolo di amicizie, conoscenze sui media sociali e così via. Dopodiché compilano delle liste di obiettivi da colpire militarmente. Sono degli acceleratori, svolgono un lavoro che prima svolgevano le agenzie di intelligence insieme a Forze armate e agenzie militari, ma lo fanno con una velocità straordinaria. Un esempio: il capo dell'esercito di un paese importante, insomma, che non voglio citare, l'anno scorso in un'intervista spiega il senso di questa cosa. Dice: noi prima producevamo 50 obiettivi all'anno, la macchina produce 100 obiettivi al giorno, e 50 di questi li colpiamo.

Quali sono le criticità? Primo: la risposta secca è no, la macchina non

sbaglia, salvo che non ci sia un guasto tecnico o che non sia stata manipolata a sua volta da un attore ostile o da un concorrente. La macchina non sbaglia. La macchina fa il suo lavoro, cioè fornisce delle risposte in base al proprio algoritmo e alle modalità di programmazione. Quali sono quindi gli eventi imprevisti che si verificano? A cosa sono dovuti? Primo, sono dovuti a delle incertezze inoculate nel sistema. Il sistema, per esempio, sa distinguere l'immagine di un miliziano con un fucile da quella di un bambino con un bastone. Sì o no? Se non lo sa distinguere, può uccidere un bambino; è potenzialmente un crimine di guerra. Secondo, distingue i colori, la posizione degli oggetti. I sistemi di posizionamento globale (GPS) sono imprecisi: una minima differenza può condurre a un attacco su un ospedale invece che su una caserma, oppure su una riunione di bambini all'asilo invece che su un centro di addestramento di miliziani.

Secondo, le presunzioni (*assumptions*): il sistema opera delle presunzioni che gli sono state insegnate dal programmatore. Per esempio, se un oggetto arriva verso la mia direzione al di sopra di questa velocità, è un attacco nei nostri confronti. Al di sopra di 300 nodi, è un attacco nei nostri confronti. Queste presunzioni a volte sono sbagliate, in particolare quando riguardano esseri umani, perché a questi sistemi, in diversi conflitti, viene insegnato a stabilire un grado, un *ranking* di pericolosità, oppure di caratteristiche che sono quelle del nemico, sulla base di una serie di elementi. Per esempio, io cambio spesso cellulare per motivi professionali; è un indice del fatto che sono un miliziano. Tutti noi che abbiamo esperienza di indagini di criminalità organizzata sappiamo che è una modalità che esiste da 35 anni, da quando ho cominciato a lavorare; è un indice. L'altro è l'uomo: le donne, in genere, vengono escluse. Un altro, l'età: se ha sopra i 60 anni, probabilmente non è un miliziano; se ha di meno, può esserlo. Qual è il circolo dei suoi amici? Ha lavorato con qualcuno che è vicino a quel gruppo? Sì o no? Nei suoi contatti telefonici c'è qualcuno che è un militare, un agente di intelligence, un miliziano nemico? Sì o no?

Sulla base di queste presunzioni viene effettuato e, se io, sfortunatamente, entro in queste condizioni ma non sono assolutamente un miliziano, non sono un militare, non sono un agente di intelligence, posso essere colpito. Di nuovo, la responsabilità non è della macchina ma di chi l'ha programmata. Terzo, il sistema ha dei preconcetti, dei pregiudizi (*bias*) e i preconcetti. Anche questi sono instillati dal programmatore. Un preconcetto può essere quello del sesso: è uomo; può essere quello dell'essere nato in una certa zona. Io sono siciliano, sono catanese, sono nato in una zona ad alta densità mafiosa, può essere un *bias* per cui io acquisto un punto o perdo in realtà un punto nel *ranking*.

Una difficoltà è quella, quindi, che riguarda la programmazione. Un'altra è quella del tempo che ha a disposizione l'operatore per accettare la proposta del sistema. Secondo inchieste giornalistiche, assolutamente non verificabili, ma comunque verosimili, in molti di questi casi il tempo a disposizione dell'operatore è di pochi secondi, a volte di qualche minuto. In quel tempo, l'operatore normalmente non è in grado di valutare se il sistema ha operato correttamente, cioè se l'obiettivo di cui ha accettato l'eliminazione è un civile, è un militare, è un oggetto civile, un'abitazione, un ospedale, una scuola, un'università. Sì o no?

Tutte queste questioni portano a una serie di conseguenze giuridiche. Primo, quali crimini si possono ipotizzare? Diversi crimini di guerra: attacco intenzionale contro beni o persone civili oppure attacchi tali da causare danni cosiddetti incidentali, collaterali. E questi sono due dei crimini che vengono a mente.

Terzo elemento determinante è quello della cosiddetta "*Policy for casualties*" (politica per le vittime). Qual è il tasso accettabile di danno incidentale? Cioè, quanti innocenti può portarsi nella tomba il mio nemico? 1, 2, 10, 100? In base a questa indicazione cambia radicalmente lo scenario, perché il diritto dei conflitti armati ruota attorno a tre principi.

Il primo, quello di distinzione, prevede che occorra distinguere soggetti verso cui si può legittimamente indirizzare la forza armata e soggetti nei confronti dei quali questo non si può fare. E sono sostanzialmente i principi delle Convenzioni di Ginevra: civili e combattenti fuori combattimento, che non sono più in grado di esercitare attività armate.

Il secondo principio è di proporzionalità: l'attacco deve essere tale, con una prognosi ex ante, in concreto, quindi con una valutazione che viene effettuata mettendosi nei panni di chi decide nel momento in cui decide, in modo tale da non determinare dei danni accidentali sproporzionati rispetto al vantaggio militare. Naturalmente, nel caso di conflitti protratti, oppure di situazioni protratte, quello che è avvenuto nei casi precedenti ha un significato, perché io so già che cosa succede, o ad esempio rispetto ai conflitti che avvengono in ambienti urbani, in cui è molto più difficile distinguere.

Il principio fondamentale, però, è quello di precauzione: devono per queste due ragioni adottare delle modalità tali da evitare i danni incidentali. Ed è un processo che tendenzialmente deve andare verso lo zero, deve tendere verso zero danni incidentali.

Un altro punto fondamentale da tenere in considerazione è che l'eventuale violazione del diritto internazionale da parte del nemico non legittima una violazione da parte dell'altro belligerante: come dire, immoralità opposte, illegalità opposte non si compensano, si sommano.

Altro esempio, e poi mi avvio verso la conclusione: ci sono dei sistemi basati anche questi su algoritmi, su intelligenze artificiali, che permettono la sorveglianza di massa. Sono utilizzati in diverse autocrazie, ma non solo, e permettono, sulla base di dati biometrici, dell'iride, della forma del volto, anche del modo in cui ci si muove, di controllare gli spostamenti di masse di persone, anche di milioni di persone, ed eventualmente di impedire a queste persone di andare in certi luoghi, o in certe parti di una città, o in certe città.

Questi possono essere, se sono basati su criteri arbitrari, crimini contro l'umanità di persecuzione su base etnica, religiosa, politica, oppure anche di apartheid, quindi all'interno di regimi che arbitrariamente distinguono le persone in base a caratteristiche personali.

Ultimo esempio, e vado alle conclusioni che tocco solo incidentalmente, è quello dell'utilizzo, anche attraverso strumenti cibernetici, di oggetti di uso comune come strumenti di guerra. Tipicamente, il cellulare, che va sempre con noi. Se il cellulare viene utilizzato fisicamente, oppure attraverso dei sistemi informatici in modo da diventare, per esempio, un oggetto esplosivo, questa è una modalità di guerra vietata, perché esiste un protocollo internazionale che è stato ratificato da moltissimi stati che vieta l'uso di queste trappole, chiamate in inglese "*booby traps*".

Concludo. Lo sviluppo tumultuoso e inarrestabile, soprattutto degli ultimissimi anni, delle tecnologie che riducono lo spazio di controllo umano e aumentano le modalità di controllo sulla vita delle persone, comporta una serie di sfide giuridiche, etiche e politiche. Nel settore di cui io mi occupo, e del quale sto trattando, non esiste un problema di mancata regolazione. Il diritto internazionale esiste, esistono le norme, sono le norme del diritto internazionale dei diritti umani che proteggono i diritti fondamentali, e le norme del diritto internazionale umanitario che regolano le modalità e i mezzi legittimi dei conflitti armati e i soggetti che possono essere destinatari legittimamente della violenza armata.

Quindi, le regole esistono, non c'è un tema di vuoto normativo. Però, come prima accennava il prefetto Guidi, andando a Kelsen, l'attuazione del diritto internazionale naturalmente è rimessa agli Stati, perché il diritto internazionale opera in questo mondo di Stati, è creato dagli Stati, e gli Stati, per fortuna, non possono facilmente modificarlo o distruggerlo per via dell'uso della consuetudine cui si riferiva prima Giovanni Salvi. Però possono, con le loro condotte, rafforzare le norme del diritto oppure svuotarle di significato.

Il tema è essenzialmente politico, perché le regole sono delle regole giuridiche, ma anche delle regole morali. Il Papa, alcuni giorni fa, rispondendo a una domanda, ha detto una cosa molto azzeccata: "La guerra è sempre

immorale, ma c'è una certa moralità anche nella guerra". La moralità sono le regole del diritto internazionale umanitario.

In questi giorni, in questi mesi, negli ultimi anni, sentiamo dire che il modo in cui i conflitti oppure le situazioni di persecuzione e all'interno degli Stati vanno avanti negli ultimi anni indicano un difetto, un errore, un fallimento del diritto internazionale. Credo che questo approccio sia errato. Il diritto è lì, le regole sono lì, il fallimento è un fallimento politico. Sono gli Stati che devono attuare il diritto internazionale. Diritto e politica stanno e cadono insieme, ma se cade il diritto internazionale, cade la politica, e soprattutto cade il dovere della politica, che è quello di comporre le controversie pacificamente e, quando è necessario, condurre le azioni armate all'interno dei binari stabiliti dal diritto e, soprattutto, di limitare quella tendenza all'estremo che era stata teorizzata da Clausewitz in un passo antecedente a quello famoso della guerra politica come altri mezzi.

Clausewitz diceva che la guerra tende all'estremo, perché i belligeranti si danno delle sfide che fanno alzare il livello fino all'incontro col dovere della politica. Ed è questo, credo, il tema fondamentale. Ed è una delle ragioni per cui questo incontro è particolarmente importante e per cui noi, con pochi mezzi, con modestia e rendendoci conto di essere soltanto uno degli anelli di un sistema molto complesso, abbiamo il dovere di fare da arbitri, di fischiare quando ci sono le infrazioni e, quindi, di indicare quando il diritto internazionale, soprattutto quello che riguarda le persone umane, viene violato.

SECONDA SESSIONE

CYBERSPAZIO. IL GRUPPO DI LAVORO APERTO DELLE NAZIONI UNITE. LA CONVENZIONE ONU SUI CRIMINI INFORMATICI NELLA COOPERAZIONE GIUDIZIARIA

CYBERSPAZIO. IL GRUPPO DI LAVORO APERTO DELLE NAZIONI UNITE. LA CONVENZIONE ONU SUI CRIMINI INFORMATICI NELLA COOPERAZIONE GIUDIZIARIA

SALUTI ISTITUZIONALI

Antonio Tajani

Vice – Presidente del Consiglio dei Ministri, Ministro degli Affari Esteri e della Cooperazione Internazionale

Sono lieto di ospitare al Ministero degli Esteri questo importante appuntamento, che offre l'opportunità di approfondire le sfide legate allo spazio virtuale. Saluto la Fondazione Vittorio Occorsio e tutti i partecipanti.

Le sfide del mondo cibernetico hanno ormai conseguenze tangibili sul mondo reale; per questo motivo è sempre più imperativo condividere ogni sforzo per contrastare le minacce. Fare squadra è cruciale. Il governo è in prima linea sul tema della sicurezza, che abbiamo reso prioritario in Europa e nel G7. Abbiamo adottato numerose misure per affrontare il tema a 360° e rafforzato il coordinamento internazionale in questo ambito strategico.

Ho anche voluto istituire presso il Ministero degli Esteri un'unità per l'innovazione tecnologica della sicurezza. Nella riunione dei ministri degli Esteri del G7 che ho presieduto a Capri, ad aprile, abbiamo affermato con forza l'importanza cruciale di assicurare che l'intelligenza artificiale sia affidabile e in linea con i nostri valori etici, mantenendo al centro la persona e i diritti umani. Questa importante sfida può trasformarsi in una grande opportunità per le nostre società e per le imprese, favorendo la crescita.

Le parole del Santo Padre al vertice G7 in Puglia sono una perfetta rappresentazione di questo nostro approccio, che anima anche il disegno di legge adottato in aprile dal governo e attualmente in discussione in Parlamento. Cruciali sono le implicazioni di sicurezza, in particolare sul tema della disinformazione, che introduce una variabile molto sensibile all'interno delle nostre società, soprattutto in un momento in cui i nostri valori sono in gioco di fronte alle autocrazie.

A questo proposito, ho firmato con il Segretario di Stato americano, Antony Blinken, a Capri, un importante accordo per rafforzare la collaborazione con gli Stati Uniti nel contrasto alla disinformazione. Appuntamenti come quello odierno dimostrano quanto possa essere fruttuosa la collabora-

zione tra diplomazia e magistratura per affermare l'esercizio della giurisdizione e la protezione dei diritti nello spazio virtuale.

Contate su di me, contate su Antonio Tajani.

PRESIEDE

Stefano Mogini
Segretario generale della Corte di Cassazione

Buongiorno a tutti. Permettetemi di ringraziare, in primo luogo, la Fondazione Occorsio per l'invito e per la ricchezza dei nostri lavori, soprattutto per la capacità di onorare l'esempio civico di Vittorio Occorsio, sollecitando analisi di alto livello sui temi più rilevanti per le nostre società, e per la sua capacità di federare tante istituzioni a livello nazionale, sovranazionale e internazionale su questi temi.

Permettetemi poi di dare una testimonianza anche della capacità della Fondazione di essere presente, di assicurare un lievito particolare lì dove si formano le menti e le coscienze dei giovani del nostro paese. Come dicevano ieri ai rappresentanti della Fondazione, ci vuole intelligenza e coraggio. Ho negli occhi ancora, per esempio, le iniziative realizzate proprio alla Corte di Cassazione dalla Fondazione Occorsio con la partecipazione di tanti giovani delle scuole, compresa quella dell'Istituto Tecnico di Caivano, che anche ieri era presente qui per ricordare l'importanza del rispetto della legalità, delle regole e dell'impegno per il bene comune.

Quindi, grazie alla Fondazione per tutto questo. Vorrei anche ringraziare per l'occasione che mi è data di tornare in questa casa, alla Farnesina, che tanta parte ha avuto nel mio percorso professionale e umano, nel corso del quale ho avuto il privilegio di servire per diversi anni presso l'Ambasciata d'Italia a Parigi quale magistrato di collegamento, e poi per sei anni a New York presso la Rappresentanza Permanente d'Italia alle Nazioni Unite come *Legal Advisor.*

È un›amministrazione, il Ministero degli Esteri, dalla quale ho imparato molto e per la quale nutro sincera gratitudine e grande ammirazione. Porto il saluto anche della Prima Presidente della Corte di Cassazione, Margherita Cassano, che è impegnata in missione all›estero ma che segue con grande interesse e vicinanza tutte le attività.

Le attività della Fondazione stamattina concentreranno la nostra attenzione sugli sforzi realizzati nel foro internazionale globale per eccellenza, l'Organizzazione delle Nazioni Unite, per sviluppare un quadro legale internazionale, una disciplina multilaterale dello spazio virtuale.

La nostra attenzione sarà focalizzata sull'adozione della Convenzione delle Nazioni Unite sui crimini informatici. Per fare questo, possiamo contare

su esperti di altissimo livello che sono stati protagonisti di questi sforzi, in ruoli importanti e in rappresentanza di posizioni nazionali o di gruppi non sempre coincidenti.

Sarà interessante conoscere la loro valutazione sia dei processi negoziali sia dei risultati che questi processi negoziali hanno prodotto o di quelli che si auspica possano essere raggiunti nei lavori futuri.

LAVORI E POTENZIALI SVILUPPI DELL'OEWG DELLE NAZIONI UNITE SULLA DISCIPLINA DELLO SPAZIO VIRTUALE

Michele Giacomelli

Inviato Speciale del Ministero degli Affari Esteri e della Cooperazione Internazionale per la cybersicurezza

Desidero innanzitutto ringraziare di cuore la Fondazione Vittorio Occorsio.

Mi è stato chiesto di parlare di "Lavori e potenziali sviluppi dell'OEWG delle Nazioni Unite (*Open Ended Working Group on Security of and in the use of Information and Communications Technologies*) sulla disciplina dello spazio virtuale", un tema che mi fa piacere approfondire con voi perché estremamente attuale.

Il Presidente dell'OEWG ha appena presentato una bozza di Risoluzione al Primo Comitato per l'approvazione del terzo rapporto annuale sullo stato di avanzamento approvato nella sessione di luglio.

Credo sia importante iniziare con una breve panoramica storica di come le norme e le regole che governano questo settore si siano evolute dalla fine del secolo scorso - quando sembrava che la rapida proliferazione delle tecnologie dell'informazione e della comunicazione (TIC) portasse alla necessità di una regolamentazione globale in materia di cibernetica, dal momento che queste tecnologie ponevano sempre più nuove minacce alla sicurezza internazionale.

La creazione del Gruppo di esperti governativi delle Nazioni Unite (UNGGE) risale al 2004. Sebbene i progressi iniziali siano stati limitati, i membri del gruppo si sono gradualmente ampliati rispetto ai 15 Stati iniziali e sono stati prodotti tre rapporti chiave nel 2010, 2013 e 2015. Nel 2018, a seguito di un'iniziativa guidata dalla Federazione Russa, l'Assemblea Generale delle Nazioni Unite ha istituito con una risoluzione l'OEWG con l'obiettivo di coinvolgere i più ampi membri delle Nazioni Unite, in particolare i Paesi in via di sviluppo, nell'affrontare le questioni legate al cyber.

L'OEWG ha pubblicato il suo primo rapporto nel 2021 e il suo mandato è stato successivamente esteso per altri cinque anni (2021-2025), mentre il mandato attuale scadrà l'anno prossimo. È in corso un dibattito su come proseguire il regolare dialogo istituzionale, rinnovando il mandato dell'OEWG o sostituendolo con un Programma d'azione (PoA), come sostenuto da molti Stati occidentali, nel tentativo di rendere gli sforzi del gruppo più orientati

all'azione, aperti al contributo di più parti interessate e in grado di affrontare diversi temi in modo trasversale.

Al centro di queste discussioni ci sono sfide di lunga data: opinioni divergenti sui modi per garantire un comportamento responsabile degli Stati nel cyberspazio e interpretazioni diverse su come il diritto internazionale si applichi a questo dominio, che la NATO definisce "quinto dominio", oltre a terra, aria, mare e spazio.

Esiste una netta divisione tra gli Stati occidentali (l'UE e quelli che la pensano allo stesso modo) e un piccolo numero di altri Stati, guidati dalla Federazione Russa. Il grande gruppo di Stati che compongono la cosiddetta terra di mezzo tende a non schierarsi. Possono offrire proposte costruttive (come la richiesta del Brasile di una moratoria sulle risoluzioni del Primo Comitato o la proposta dell'India di un portale per coordinare gli sforzi di sviluppo delle capacità informatiche).

Gli Stati occidentali, in generale, ritengono che l'attuale quadro normativo sia adeguato a regolare il cyberspazio e prevenire i conflitti. Sostengono che il quadro giuridico internazionale esistente sia sufficiente, senza grandi lacune. La posizione fondamentale è che il cyberspazio non è privo di leggi. Le leggi e le norme che regolano altri domini possono e devono essere applicate anche al cyberspazio. Sebbene la possibilità di creare nuove norme non sia del tutto esclusa, tali passi dovrebbero essere presi in considerazione solo dopo un'approfondita revisione e valutazione delle lacune e delle differenze interpretative esistenti.

Al contrario, un numero significativo di Stati sostiene che il cyberspazio è unico e che le norme create per altri contesti non possono essere semplicemente trasposte. Per questo motivo, chiedono la creazione di una convenzione giuridicamente vincolante specifica per il dominio cibernetico. Questo rimane un punto chiave di divergenza.

Molti temono, come hanno notato diversi osservatori e ricercatori, che la richiesta di nuove norme possa essere una strategia per eludere il quadro attuale. Si teme che una convenzione di questo tipo possa indebolire le restrizioni esistenti, in particolare per quanto riguarda gli attori non statali, spesso responsabili di attività dannose. In realtà, il dibattito è politico oltre che giuridico.

Quali sono gli elementi che compongono il quadro sopra citato?

Si tratta di una combinazione di norme vincolanti generali, basate su trattati e consuetudini, mutuate dal mondo cinetico e applicate per analogia al cyberspazio. A queste si aggiungono le 11 norme volontarie e non vincolanti adottate nel 2015 dall'UNGGE (*Unite Nations Group of Governmental Experts*) sul comportamento responsabile degli Stati.

È ormai ampiamente accettato che la Carta delle Nazioni Unite e i principi del diritto internazionale si applicano al ciberspazio. Il punto controverso non è se il diritto internazionale si applica al cyberspazio, ma come si applica.

Diversi principi chiave sono al centro di questo dibattito, tra cui:

- la sovranità dello Stato, che può essere violata anche senza l'uso illegale della forza;
- il non intervento, dove l'uso non autorizzato di sistemi TIC all'interno del territorio di uno Stato può essere considerato un intervento illegale se la portata e gli effetti sono paragonabili a quelli di interventi non informatici;
- l'uso della forza, la minaccia o l'uso della forza contro l'integrità territoriale e l'indipendenza di un altro Stato, come indicato nell'articolo 2(4) della Carta delle Nazioni Unite, principio che si basa sul concetto di soglia, oltre la quale l'uso della forza è considerato avvenuto; in questo contesto, la misura più affidabile sembra essere quella degli effetti della forza utilizzata, e ciò, in particolare, se la portata e l'impatto di un attacco informatico, in corso o minacciato, siano paragonabili a quelli di un'azione militare cinetica;
- il diritto all'autodifesa, che implica la valutazione del superamento della soglia di un attacco armato, come definito dall'articolo 51 della Carta delle Nazioni Unite, e di conseguenza della proporzionalità e della necessità della risposta;
- la responsabilità dello Stato, che è questione estremamente delicata, poiché implica il processo di attribuzione; in pratica, è necessario stabilire la responsabilità dello Stato in modo chiaro e definitivo; nel mondo di oggi, questo non è facile: le attività malevole sono condotte principalmente da attori non statali, la cui natura granulare rende difficile collegarle definitivamente a uno Stato specifico; per questo motivo il processo di attribuzione è così complesso; è comune distinguere tra attribuzione tecnica e attribuzione politica per evidenziare la complessità del processo e per sottolineare che, in ultima analisi, la decisione di attribuire attività malevole a uno Stato rientra sempre nella competenza sovrana di un altro Stato ed è guidata principalmente da considerazioni politiche. A causa di questa complessità, non è ancora stata definita una soglia precisa per stabilire quando un'attività cibernetica costituisca uso della forza. Le attribuzioni pubbliche di responsabilità, come abbiamo visto negli ultimi tempi, sono spesso respinte dagli Stati accusati in quanto politicamente motivate e non basate su prove convincenti; se da un lato la comunità internazionale condanna ampiamente i comportamenti dolosi, in

particolare quelli che prendono di mira infrastrutture critiche o settori sensibili come la sanità e l'energia, dall'altro è necessario comprendere in modo pragmatico quali risultati tangibili ci si possa realisticamente aspettare solo da un esercizio di attribuzione di colpe;

- contromisure: dipendono dall'identificazione della responsabilità dello Stato aggressore. Nel mondo cibernetico sono soggette alle stesse limitazioni del mondo non cibernetico, tra cui la proporzionalità, l'ottenimento di risarcimenti e la trasparenza;
- Due diligence: gli Stati sono obbligati a garantire che il loro territorio non sia consapevolmente utilizzato per condurre attività informatiche che violino i diritti di altri Stati. Il principio generale della dovuta diligenza implica anche l'adozione di ragionevoli misure preventive, che possono richiedere a ciascuno Stato un livello minimo di infrastrutture ITC e di capacità di governance. In sostanza, si tratta di un obbligo di condotta, non necessariamente di risultato;
- Risoluzione pacifica delle controversie, principio che si estende alle controversie che coinvolgono le attività informatiche tra Stati;
- Rispetto dei diritti umani: secondo l'interpretazione prevalente, il diritto internazionale dei diritti umani si applica alle attività informatiche nello stesso modo in cui si applica al di fuori del contesto informatico, sia online che offline. I cittadini hanno gli stessi diritti e gli Stati sono tenuti a garantire il rispetto dei diritti umani;
- In linea con il diritto internazionale umanitario (DIU), è generalmente accettato che, in caso di conflitto armato, il DIU si applichi al dominio cibernetico. Tuttavia, durante l'ultima sessione dell'OEWG, la Russia e altri Stati si sono opposti alla menzione esplicita del diritto internazionale umanitario nel testo.

Le simulazioni basate su scenari, costruite su incidenti e risposte ipotetiche, organizzate da organizzazioni internazionali come l'UNIDIR o da istituti di ricerca, si sono rivelate utili per favorire la comprensione reciproca. Altrettanto importanti sono le posizioni nazionali sull'applicazione del diritto internazionale che alcuni Stati (anche se non molti) hanno pubblicato negli ultimi anni. L'Italia, ad esempio, ha condotto uno studio approfondito nel settembre 2021, grazie a una collaborazione tra il MAE, la Presidenza del Consiglio dei Ministri e il Ministero della Difesa. L'UE ha preparato una posizione comune che dovrebbe integrare, non sostituire, le posizioni nazionali.

In questo contesto, vorrei citare anche il Tallinn Manual, un documento accademico pubblicato per la prima volta nel 2013 dall'Università di Cambridge, su iniziativa del *NATO Cooperative Cyber Defence Centre of Excellence*. Inizialmente, il testo si concentrava principalmente sulle situazioni di *jus*

ad bellum, tipiche del contesto dei conflitti armati. Nel 2017 è stata pubblicata una versione aggiornata del manuale, che ha ampliato il suo campo di applicazione alle norme di diritto internazionale che regolano gli incidenti informatici che gli Stati incontrano. Il Manuale di Tallinn, insieme ad altre pubblicazioni simili, costituisce un riferimento autorevole per l'interpretazione del diritto internazionale nel cyberspazio.

Finora abbiamo discusso le norme generali dei trattati e quelle consuetudinarie. A queste si aggiungono le 11 norme non vincolanti sul comportamento responsabile degli Stati, altro elemento essenziale del quadro. Queste norme forniscono linee guida per indirizzare le azioni degli Stati e valutarne la conformità. Tre delle norme riguardano divieti su ciò che gli Stati non devono fare: non devono permettere che dal loro territorio vengano condotte attività dannose, non devono danneggiare le infrastrutture critiche e non devono danneggiare le squadre di pronto intervento. D'altra parte, le restanti otto norme si concentrano su azioni positive: gli Stati devono lavorare per promuovere la cooperazione e rispondere alle richieste di assistenza. Queste norme sono esaustive o sono soggette a evoluzione? La sintesi del presidente dell'OEWG nella sessione del luglio 2024 è stata che entrambi i percorsi dovrebbero continuare. Cito dal Rapporto Annuale sui Progressi (APR): "L'OEWG deve, agendo su base consensuale, continuare, in via prioritaria, a sviluppare ulteriormente le regole, le norme e i principi del comportamento responsabile degli Stati e le modalità della loro attuazione e, se necessario, introdurre modifiche ad essi o elaborare ulteriori regole di comportamento". Per promuovere una maggiore convergenza, la presidenza, sostenuta dagli Stati membri, ha sviluppato una Checklist volontaria di azioni pratiche (per l'attuazione delle norme di comportamento responsabile degli Stati nell'uso delle TIC). Questa lista di controllo è considerata un documento vivo, nel senso che è destinata ad evolversi nel tempo.

Ma la vera domanda rimane: queste 11 norme volontarie vengono applicate o no? E se non lo sono, perché? Quali meccanismi sono in atto per incoraggiare gli Stati ad applicarle? La comunità internazionale ha ancora molta strada da fare per trovare risposte definitive a queste domande.

Oltre a queste questioni centrali, il mandato dell'OEWG comprende anche diversi argomenti interconnessi, tra cui:

- Identificare le minacce nuove e tradizionali: mentre i rischi convenzionali per le infrastrutture critiche rimangono una priorità, ora stiamo affrontando anche sfide emergenti come il ransomware, le applicazioni di intelligenza artificiale, le criptovalute e la tecnologia quantistica;
- Misure di rafforzamento della fiducia (CBM): sono essenziali per evitare che gli Stati siano colti di sorpresa o interpretino male le azioni reciproche; nel marzo 2024, l'ONU ha lanciato una nuova *PoCs Directory* (il registro dei punti di contatto all'interno dell'ONU), uno strumento volontario progettato per migliorare la comunicazione e la cooperazione, sulla base di sforzi analoghi dell'OSCE; in questo ambito, le organizzazioni regionali svolgono un ruolo significativo, come l'OSCE, che ha approvato 16 CBM (l'Italia ha sponsorizzato il numero 14, sui partenariati pubblico-privati);
- *Cyber Capacity Building* (CCB): questa iniziativa mira ad aiutare gli Stati a rafforzare la loro resilienza politica e tecnica, consentendo loro di difendersi e rispondere efficacemente alle minacce informatiche; recenti discussioni si sono incentrate sulla creazione di un portale delle Nazioni Unite per aggregare tutte le iniziative di sviluppo delle capacità e sulla potenziale creazione di un fondo CCB dedicato, possibilmente aperto a contributi privati;
- Dialogo istituzionale: oltre al dibattito tra OEWG e PoA, la questione riguarda anche l'inclusione di stakeholder non statali e, di conseguenza, il rapporto con il settore privato (Russia e Cina cercano di limitare questo aspetto e di sottolineare la natura intergovernativa del processo).

In conclusione, la regolamentazione del cyberspazio è profondamente influenzata dal più ampio contesto geopolitico. Di conseguenza, il dibattito è caratterizzato da una significativa polarizzazione. La divisione tra la creazione di una nuova convenzione e l'attuazione delle norme esistenti, così come tra un approccio intergovernativo e un modello "*multi-stakeholder*", riflette una fondamentale mancanza di fiducia reciproca e visioni del mondo divergenti.

Naturalmente il dialogo e la discussione sono essenziali, ma trovare un terreno comune rimane una sfida. Ciò è stato evidente nei recenti negoziati in

seno alle Nazioni Unite sulla Convenzione sulla criminalità informatica e per la finalizzazione del Patto digitale globale, adottato nelle scorse settimane durante il segmento ministeriale dell'Assemblea generale delle Nazioni Unite, insieme al Patto per il futuro.

Tuttavia, se abbiamo una prospettiva di decenni più che di anni, possiamo affermare che i progressi sono possibili. In definitiva, il percorso verso il multilateralismo non è mai semplice, e il ciberspazio non fa eccezione. Dobbiamo continuare a impegnarci su questi temi critici, facendo leva su prospettive e competenze diverse. È fondamentale coinvolgere un'ampia gamma di professionisti e parti interessate in questo dialogo continuo.

Grazie per la vostra attenzione.

COME RENDERE EFFICACE LA COOPERAZIONE GIUDIZIARIA MULTILATERALE IN MATERIA DI CRIMINALITÀ INFORMATICA: UNA PROSPETTIVA MULTIFORME SUL CYBERSPAZIO

Eric Do Val Lacerda Sogocio

Vicepresidente del Comitato ad hoc per l'elaborazione di una Convenzione internazionale sulla criminalità informatica. Già Capo della Divisione contro la criminalità transnazionale, Consigliere del Ministero degli Affari Esteri del Brasile

Vorrei innanzitutto ringraziare la Fondazione Vittorio Occorsio e la Presidenza del Consiglio dei Ministri per avermi invitato qui oggi. Come ho detto a Giovanni Salvi durante i preparativi di questa conferenza, è un onore vedere il mio nome elencato tra un gruppo così eminente di professionisti e accademici che si occupano di diversi aspetti del cyberspazio.

Sono inoltre entusiasta di condividere questo panel con Stefano Mogini, Michele Giacomelli, Luigi Birriteri, Glen Prichard, Antonio Balsamo e soprattutto l'ambasciatore Deborah McCarthy, eccellente partner negli ultimi anni durante i negoziati della Convenzione delle Nazioni Unite contro la criminalità informatica.

C'è una ricca storia dietro il lungo e intrigante titolo della Convenzione e, se il tempo a disposizione lo permetterà, potremo approfondirla durante il dibattito.

Oggi propongo di:

1. Discutere la questione della giurisdizione dal punto di vista della cooperazione internazionale nella lotta alla criminalità informatica, sostenendo che la criminalità informatica dovrebbe essere affrontata separatamente a causa delle sue caratteristiche uniche.
2. Esaminare gli aspetti chiave della Convenzione delle Nazioni Unite e il modo in cui essa consente ai Paesi di rafforzare la resilienza contro le sfide internazionali, migliorando così la sicurezza nazionale e la sicurezza dei cittadini.
3. Condividere le informazioni sull'approccio del Brasile alla giurisdizione in materia di acquisizione di prove e di rapporti con i fornitori di servizi.

Innanzitutto, perché la cooperazione internazionale nella lotta alla criminalità informatica dovrebbe essere trattata in modo diverso da altre questioni informatiche come la sicurezza informatica, la difesa informatica o la governance del cyberspazio?

In sostanza, le giurisdizioni nazionali – o le sovranità – cooperano solo se decidono di farlo. Non esiste un meccanismo che costringa un Paese a cooperare contro la sua volontà.

Si consideri un esempio tratto dalla "Proposta di Evento Collaterale" che ha guidato la preparazione di questa conferenza:

"Un attacco hacker a strutture strategiche può costituire contemporaneamente un crimine, punibile penalmente, e un'aggressione alla sovranità nazionale. Quest'ultima può costituire una violazione del Diritto Internazionale (IL) e del Diritto Internazionale Umanitario (DIU), le cui conseguenze e reazioni sono disciplinate dagli strumenti di tale corpus normativo".

Supponiamo che le autorità del Paese colpito considerino l'attacco come un crimine e intendano perseguire gli autori. Hanno bisogno di un reato chiaramente definito, di un sospetto identificato, di prove ammissibili e di un legame dimostrabile tra l'atto e l'individuo. L'intelligence da sola non è sufficiente; spesso sono necessarie prove concrete, come nel caso del sistema giuridico brasiliano.

Se il sospetto risiede in un'altra giurisdizione, le autorità devono richiedere formalmente l'assistenza di quella giurisdizione per ottenere le prove necessarie. Questa cooperazione si basa tipicamente su accordi bilaterali di assistenza legale reciproca, su convenzioni internazionali come la Convenzione di Palermo o la Convenzione di Budapest, o sulla semplice reciprocità. Un fattore critico in questo caso è la doppia incriminazione: i Paesi forniranno assistenza se la condotta è criminale in entrambe le giurisdizioni.

Tuttavia, se l'altro Paese sceglie di non collaborare, il processo si blocca. Il rifiuto può essere giustificato da una serie di ragioni, che vanno da motivi legali sostanziali a tecnicismi procedurali come la formattazione dei documenti. Pertanto, la cooperazione legale internazionale nel perseguire i crimini informatici dipende interamente dalla volontà reciproca.

Questa sfida è stata evidente durante i negoziati della Convenzione delle Nazioni Unite contro la criminalità informatica. La bozza iniziale diffusa dalla Russia confondeva i concetti affrontando difesa, sicurezza e criminalità in un unico strumento. Paesi come il Brasile hanno espresso riserve su questo approccio. Fortunatamente, con il progredire dei negoziati, l'attenzione si è ristretta alla criminalità informatica, consentendo l'adozione anche in un clima internazionale difficile.

Un'altra idea sbagliata era che una convenzione multilaterale potesse obbligare i Paesi a cooperare. In realtà, la convenzione fornisce definizioni condivise dei reati, soddisfacendo il requisito della doppia criminalizzazione, e offre strumenti di cooperazione ai Paesi che lo desiderano.

La cooperazione implica l'impegno con le controparti, non con gli avversari. Si tratta di riconoscere, non di affermare, le sovranità. Ciò è in linea con la filosofia africana dell'Ubuntu: "Io sono perché tu sei". Pertanto, la lotta alla criminalità informatica attraverso la cooperazione internazionale rafforza le giurisdizioni e le sovranità.

Questo approccio basato sul partenariato distingue la criminalità informatica da altri domini informatici. Quando le sovranità si contrappongono, le questioni rientrano nella cybersecurity o nella cyberdifesa e richiedono strategie diverse, come l'attribuzione e la promozione di un comportamento responsabile degli Stati nel cyberspazio. In secondo luogo, la Convenzione delle Nazioni Unite fornisce una base alle giurisdizioni per criminalizzare atti specifici e facilita un'efficace cooperazione internazionale.

La Convenzione delinea i reati dipendenti dal cyberspazio che gli Stati membri dovrebbero adottare a livello nazionale:

- Accesso illegale
- Intercettazione illegale
- Interferenza con i dati elettronici
- Interferenza con i sistemi di tecnologia dell'informazione e della comunicazione (TIC)
- Uso improprio di dispositivi
- Falsificazione legata alle TIC
- Furto o frode legati alle TIC

Definisce inoltre i reati abilitati dall'informatica, quali:

- Materiale per abusi sessuali su minori
- Adescamento per commettere reati sessuali contro un minore
- Diffusione non consensuale di immagini intime
- Riciclaggio di proventi di reato
- Partecipazione e tentativo di attività criminali

Adottando queste definizioni, i Paesi soddisfano il requisito della doppia incriminazione, consentendo loro di richiedere e offrire cooperazione nelle indagini e nei procedimenti giudiziari.

Lo scambio tempestivo di informazioni e prove è fondamentale, vista la facilità con cui i dati possono essere alterati o cancellati nel cyberspazio. La Convenzione affronta questo problema attraverso una rete attiva 24 ore su 24, 7 giorni su 7, in ogni Stato membro, per richieste rapide. La conservazione dei dati è fondamentale, così come la possibilità di scambiare prove elettroniche per i reati più gravi, quelli che giustificano una pena massima di almeno quattro anni di reclusione, secondo la Convenzione di Palermo.

La lotta alla criminalità informatica richiede partner, non avversari. Le giurisdizioni traggono vantaggio quando tutte le controparti, non solo gli al-

leati, possono svolgere efficacemente le loro funzioni di giustizia penale. Ciò sottolinea l'importanza del rafforzamento delle capacità per evitare gli anelli deboli della catena.

Rafforzando le capacità di altri Paesi, rafforziamo la sovranità e il ruolo delle giurisdizioni a livello globale. L'obiettivo è quello di stabilire standard minimi universali di criminalizzazione per eliminare i paradisi sicuri per i criminali informatici.

Questo avvalora ulteriormente la tesi che la criminalità informatica debba essere affrontata in modo distinto da altre aree informatiche.

In terzo luogo, esaminiamo come la legislazione brasiliana gestisce la giurisdizione nell'accesso alle informazioni e alle prove.

La legge quadro civile brasiliana su Internet stabilisce che le aziende che offrono servizi in Brasile devono rispettare la legislazione brasiliana e le ordinanze dei tribunali. Questo vale indipendentemente dal luogo in cui i dati sono archiviati o dalla sede dell'azienda.

Questo approccio rafforza la giurisdizione e la sovranità nazionale, non contro altre giurisdizioni, ma a favore dei cittadini e del sistema giuridico nazionale.

Di conseguenza, il sistema giudiziario brasiliano richiede che le aziende che operano in Brasile mantengano dei rappresentanti legali all'interno del Paese, in grado di ricevere ed elaborare gli ordini del tribunale e di rispondere in caso di mancata osservanza.

Questo non è stato senza opposizione. Un caso degno di nota ha coinvolto Facebook (ora Meta), che ha presentato una petizione alla Corte Suprema per decidere sulla costituzionalità dell'accordo di cooperazione legale tra Brasile e Stati Uniti. L'obiettivo era quello di imporre che le richieste giudiziarie seguissero il lungo processo internazionale di assistenza legale reciproca, rendendo inefficace il rispetto diretto degli ordini del tribunale brasiliano attraverso i loro rappresentanti locali. La tradizionale cooperazione bilaterale rimane una via aggiuntiva, non l'unica.

Negli ultimi anni, i tribunali brasiliani hanno imposto il rispetto delle norme bloccando temporaneamente l'accesso ad applicazioni come WhatsApp e Telegram quando non hanno risposto alle richieste giudiziarie o non hanno nominato rappresentanti legali. Recentemente, X (ex Twitter) è stata sospesa per 39 giorni fino a quando non si è conformata agli ordini di rimuovere gli account, nominare un rappresentante legale e pagare le multe per la mancata conformità.

Una volta ottemperato, X ha dichiarato:

"X è orgogliosa di tornare in Brasile. Dare a decine di milioni di brasiliani l'accesso alla nostra indispensabile piattaforma è stato fondamentale du-

rante l'intero processo. Continueremo a difendere la libertà di parola, entro i limiti della legge, ovunque operiamo".

L'espressione "entro i confini della legge" sottolinea l'importanza di aderire al quadro giuridico di ogni giurisdizione, riaffermando la giurisdizione per garantire la sicurezza dei cittadini.

Tuttavia, dobbiamo essere realistici. Durante i negoziati della Convenzione ONU molti delegati hanno notato che le grandi aziende tecnologiche spesso ignorano le loro richieste. Per affermare con successo la propria giurisdizione, i Paesi devono disporre di un solido quadro giuridico nazionale, di normative efficaci e di un'influenza significativa.

In conclusione, tornando al titolo del nostro panel – "Come rendere efficace la cooperazione giudiziaria multilaterale in materia di criminalità informatica: una multiforme prospettiva sul cyberspazio" – la Convenzione delle Nazioni Unite contro la criminalità informatica, in quanto trattato multilaterale giuridicamente vincolante, consente agli Stati membri di far valere le proprie giurisdizioni in modo collaborativo in modi che sarebbero meno efficaci singolarmente

Deborah McCarthy
Ambasciatore Us presso il Comitato ad hoc per la Convenzione Onu sui crimini informatici

Buongiorno, sono molto onorata e contenta di essere stata invitata a questa importante discussione e vorrei ringraziare la Fondazione Vittorio Occorsio e il Ministero Italiano degli Affari Esteri e della Cooperazione Internazionale.

È un piacere personale tornare a Roma, dove ho trascorso tre anni e mezzo formativi all'inizio della mia carriera diplomatica come Capo di gabinetto dell'Ambasciatore americano in Italia. Da allora, ho avuto il piacere di lavorare con i miei colleghi italiani in tutto il mondo, compreso il recente successo nella conclusione di un nuovo trattato sulla criminalità informatica presso le Nazioni Unite.

Oggi, per prima cosa, fornirò una panoramica della nostra strategia nazionale di cybersecurity per contestualizzare i miei successivi commenti sul nuovo accordo dell'ONU sulla criminalità informatica.

La strategia nazionale di cybersicurezza US 2023 si basa su cinque pilastri che comprendono:

1. la difesa delle infrastrutture critiche
2. l'interruzione e lo smantellamento degli attori delle minacce,
3. la formazione delle forze di mercato per promuovere la sicurezza e la resilienza,
4. l'investimento nel futuro,
5. la creazione di partnership internazionali per perseguire obiettivi condivisi.

Ogni pilastro sottolinea la necessità di una collaborazione tra comunità diverse, tra cui il settore pubblico, l'industria privata, la società civile e gli alleati e partner internazionali.

Questo è stato un aspetto importante dell'approccio degli stati uniti ai negoziati dell'ONU sulla criminalità informatica e influenzerà il modo in cui ne monitoreremo l'attuazione. A nostro avviso, questa collaborazione è fondamentale per combattere efficacemente la criminalità informatica.

Ma torniamo alla strategia generale: è importante notare che gli Stati Uniti hanno apportato due cambiamenti fondamentali a livello nazionale nel modo in cui assegnano ruoli, responsabilità e risorse nel cyberspazio:

- Il primo è stato quello di spostare l'onere della difesa del cyberspazio dall'utente finale ai proprietari e agli operatori dei sistemi e ai fornitori di tecnologia che li costruiscono e li servono. A titolo di esempio, nel maggio 2021 il Presidente ha emesso l'Ordine Esecuti-

vo 14028, che impone ai fornitori di servizi di condividere le informazioni sugli incidenti e le minacce informatiche che potrebbero avere un impatto sulle reti governative; l'ordine ha inoltre stabilito standard di sicurezza di base per lo sviluppo dei software venduti al Governo, richiedendo tra l'altro agli sviluppatori di mantenere una maggiore visibilità sul proprio software e di rendere pubblici i dati sulla sicurezza.

- Il secondo cambiamento è stato quello di riallineare gli incentivi per favorire gli investimenti a lungo termine; il Governo ha lavorato per modificare gli incentivi, in modo da garantire che le forze di mercato e i programmi pubblici premino la sicurezza e la resilienza, abbraccino la sicurezza e la resilienza attraverso la progettazione e coordinino strategicamente la ricerca. Ciò è stato fatto in parte attraverso ordini esecutivi e memorandum presidenziali che, tra l'altro, stabiliscono i requisiti di cybersecurity in settori chiave, nonché attraverso la legislazione del congresso, come il *Chips Act*.

Ai fini della discussione odierna sulla criminalità informatica, noterò che il secondo pilastro della strategia si concentra sull'interruzione e lo smantellamento degli attori delle minacce. Sul fronte interno, ciò ha portato a un più stretto coordinamento interno attraverso: 1) l'ampliamento della capacità della *National Cyber Investigative Joint Task Force* (NCIJTF), che comprende 30 agenzie statunitensi, le forze dell'ordine e il Dipartimento della Difesa; 2) l'ampliamento dei meccanismi pubblico-privati per la condivisione di informazioni, comprese quelle di intelligence, e la collaborazione per interrompere le operazioni dannose; 3) l'attenzione al ransomware, anche attraverso una task force dedicata; è da notare la convinzione di fondo che i fornitori di servizi debbano compiere ragionevoli tentativi per proteggere l'uso delle loro infrastrutture da abusi o altri comportamenti criminali.

Il quinto pilastro della strategia si concentra sui partenariati internazionali per perseguire obiettivi condivisi, a livello multilaterale, regionale e bilaterale. Tra le nuove iniziative vi sono: la coalizione per la libertà online, il dialogo quadrilaterale sulla sicurezza tra Stati Uniti, Australia, India e Giappone, il Consiglio Stati Uniti – Unione Europea per il Commercio e la Tecnologia (c.d. TTC, *Trade and Technology Council*), l'iniziativa sul ransomware. Vi rientrano anche le discussioni in corso per un accordo USA-UE sull'accesso alle prove elettroniche nei procedimenti penali.

Il quinto pilastro prevede sforzi di cooperazione per individuare, attribuire e punire gli attori statali che violano le norme concordate di comportamento responsabile dello Stato nel cyberspazio. Inoltre, chiede sforzi interna-

zionali per rendere sicure le catene di approvvigionamento. E ancora, sottolinea l'importanza di forti coalizioni per definire norme e standard in vari forum e per contrastare gli sforzi volti a espandere il controllo statale su internet per controllare lo spazio dell'informazione.

Sulla scia dell'ascesa dell'AI, noto che questo pilastro include la partecipazione degli Stati Uniti alla Convenzione quadro del Consiglio d'Europa sull'intelligenza artificiale e i diritti umani, la democrazia e lo stato di diritto, che stabilisce una linea di base condivisa per l'utilizzo dell'AI. Un altro esempio è la recente risoluzione dell'ONU, sponsorizzata da noi e da altri paesi simili, per promuovere sistemi di intelligenza artificiale sicuri e affidabili.

Infine, il quinto pilastro contempla un forte impegno per fornire competenze, formazione e assistenza ai Paesi attraverso diverse agenzie statunitensi. Un esempio è l'ampio lavoro svolto dal Dipartimento della Giustizia in tutto il mondo per fornire formazione sulle prove digitali e assistenza tecnica per aiutare a raccogliere e utilizzare le prove elettroniche. Un altro esempio è il nuovo fondo per la sicurezza e l'innovazione tecnologica internazionale (ITSI) del mio stesso Ministero, volto a sostenere lo sviluppo e l'adozione di catene di fornitura di semiconduttori e reti di telecomunicazioni sicure. Ne parlo perché, quando pensiamo ai meccanismi di cooperazione internazionale per combattere la criminalità informatica, il ruolo del rafforzamento delle capacità, compresa l'assistenza legale per riscrivere le leggi, è fondamentale. Come abbiamo visto nei negoziati dell'AHC, è stato il desiderio di questa assistenza a spingere molti paesi ad aderire al consenso.

Dopo aver delineato il nostro approccio al cyber a livello nazionale e internazionale, vorrei soffermarmi sulla nuova Convenzione dell'ONU sulla criminalità informatica, recentemente conclusa.

Va sottolineato che quando questo processo è stato avviato nel 2017 da Russia, Cina e altri, l'obiettivo era quello di avere una Convenzione non di Budapest. Molti paesi non potevano o non volevano aderire alla Convenzione di Budapest. Nel 2019 è stata presentata una risoluzione redatta dalla Russia per avviare la discussione, alla quale gli Stati Uniti si sono opposti; la risoluzione è stata poi adottata con 88 voti favorevoli, 59 contrari e 34 astensioni.

In fretta e furia si è arrivati all'inizio dei negoziati veri e propri, nel gennaio 2022. Grazie al duro lavoro dei nostri partner e di chi la pensa come noi, abbiamo spostato l'attenzione dalla bozza russa a una bozza alternativa tratta da Budapest, UNTOC, UNCAC e alcuni accordi regionali. I negoziati sono stati difficili e non era chiaro se avrebbero avuto successo. Tuttavia, lo scorso agosto, il progetto di convenzione è stato adottato per consenso. Ci sono stati drammi e controversie fino alla fine.

Cosa è stato raggiunto tale risultato?

1. Un progetto di convenzione che, come ho notato, ha la maggior parte del suo contenuto tratto da accordi internazionali esistenti come Budapest, UNTOC e UNCAC, è stata una vittoria, visto che all'inizio Russia e Cina avevano presentato un proprio testo, molto diverso e assai ampio, che copriva questioni relative alla sicurezza informatica, alla sicurezza delle informazioni e alla governance di internet.
2. Un accordo che prevede un elenco ristretto di crimini informatici, elencando solo quelli che dipendono dal cyber, come l'accesso illegale, l'intercettazione illegale, l'interferenza con i dati elettronici, ovvero crimini che non esistevano prima dell'avvento di internet, oltre ad alcuni importanti crimini abilitati dal cyber, tra cui il riciclaggio di denaro e l'abuso/sfruttamento sessuale di minori e l'adescamento online. Siamo riusciti a impedire i tentativi di molti paesi di includere altri 20 crimini definiti in modo vago come "crimini informatici", che avrebbero potuto compromettere la libertà di parola e altre libertà. Tuttavia, è probabile che questi crimini vengano riproposti nelle discussioni su un futuro protocollo all'accordo, previsto nella risoluzione di accompagnamento.
3. Un accordo che va oltre gli strumenti internazionali esistenti per l'applicazione della legge, includendo le tutele dei diritti umani. È la prima volta che una Convenzione delle Nazioni Unite sulla giustizia penale include, ad esempio, un motivo di rifiuto contro la discriminazione. Inoltre, questo sarà il primo trattato dell'ONU che definisce il bambino come una persona di età inferiore ai 18 anni ai fini dei reati legati alle CSAM[24], che include una definizione solida e completa di CSAM e che richiede la criminalizzazione della trasmissione di CSAM, dell'accesso a CSAM online, del possesso di CSAM e dell'adescamento di bambini online.

   Faccio notare che l'accordo prevede anche la condivisione delle prove elettroniche per le indagini sui crimini gravi, la cui definizione proviene dall'UNTOC; a questi reati si applicano le garanzie e le protezioni previste dagli articoli 6, 24 e 40(22). L'obiettivo è quello di contribuire all'assistenza nei crimini per i quali esistono prove elettroniche, non solo nei crimini informatici. Rilevo anche la presenza di un articolo che riguarda la protezione dei dati personali.
4. Un accordo che, durante i tre anni di negoziati, ha portato altri paesi ad aderire a Budapest, tra cui la Nigeria e il Brasile.

---

24 CSAM è l'acronimo di Child Sexual Abuse Material (NDR)

5. E infine, un accordo a cui molti paesi piccoli e medi hanno accettato di aderire, in quanto offre loro la possibilità di adattare le proprie leggi e costruire la propria capacità di combattere la criminalità informatica. Insieme ai principali partner, abbiamo ripetutamente dichiarato di essere pronti a fornire assistenza in questo sforzo.

Cosa apporta il nuovo accordo alle nostre forze dell'ordine? Aumenterà il nostro raggio d'azione nella cattura dei criminali informatici e renderà possibile perseguire coloro che utilizzano il cyberspazio per sfruttare sessualmente i bambini. Tra gli altri elementi, la nuova convenzione: a) aggiorna automaticamente tutti i nostri vecchi trattati di estradizione per aggiungere la criminalità informatica e i reati sessuali online; b) garantisce la doppia incriminazione per questi reati, ovvero tutti gli Stati parte devono criminalizzare gli stessi reati, per cui potremo estradare da Paesi che non sono parte della Convenzione di Budapest"; c) permette di chiedere l'estradizione da Paesi con i quali non abbiamo accordi.

Quali sono i prossimi passi? Lo strumento sarà esaminato da due comitati delle Nazioni Unite prima di essere sottoposto all'approvazione dell'Assemblea generale delle Nazioni Unite; si prevede che venga approvato per consenso.

Ma il processo non finirà qui. Oltre alla firma e alla ratifica nazionale, la risoluzione di accompagnamento prevede la discussione di un possibile protocollo a partire dal 2026. Tali discussioni si concentreranno, tra l'altro, su ulteriori crimini da sottoporre all'esame della Conferenza delle Parti per l'inclusione nello strumento; sebbene la soglia per l'adozione di qualsiasi protocollo sia elevata (60 Paesi), vi sono rischi di espansione in aree che noi e i nostri partner non consideriamo crimini informatici.

Vorrei concludere parlando del ruolo della società civile, dell'industria e di altri soggetti nella lotta alla criminalità informatica.

Durante i negoziati, in virtù di una procedura originale erano presenti molte parti interessate. Hanno potuto offrire commenti, presentare proposte e altro ancora. Anche se non tutti i loro suggerimenti sono stati accolti, riteniamo che le parti interessate siano una parte essenziale del processo. Molti, in particolare attori del settore privato, sono spesso le prime vittime della criminalità informatica. Pertanto, il loro contributo all'attuazione del nuovo trattato sarà fondamentale.

Lo stesso si può dire per i molteplici gruppi per i diritti umani. Sono molto preoccupati per un nuovo strumento delle Nazioni Unite che include Stati come la Russia, la Cina e altri che hanno una definizione molto diversa di criminalità informatica e che potrebbero cercare di colpire i loro cittadini all'estero o cercare di esercitare pressione sugli Stati più deboli per condivi-

dere le informazioni. Riteniamo che in futuro dovremo avere al nostro fianco le parti interessate per monitorare l'attuazione dello strumento e per denunciare eventuali abusi da parte di alcuni governi. Nella mia dichiarazione di posizione alla fine dei negoziati, ho sottolineato che saremmo stati vigili e avremmo usato vari strumenti di potere, comprese le sanzioni in caso di abuso. Mi aspetto che ribadiremo nuovamente questa posizione.

LA COOPERAZIONE MULTILATERALE NEI CYBERCRIMES TRA NUOVA CONVENZIONE UN E SECONDO PROTOCOLLO CONVENZIONE DI BUDAPEST

Luigi Birritteri
Capo Dipartimento per gli affari di giustizia – Ministero della Giustizia

Grazie alla Fondazione Occorsio per le reiterate occasioni di approfondimento in cui è impegnata. Grazie all'opera di Giovanni Salvi in questa particolare e delicata materia. Dopo quello che è stato detto da Eric Sogocio e dall'ambasciatore, devo fare una critica al sistema americano perché davvero non comprendo come si possa consentire che l'ambasciatrice McCarthy vada in pensione prima di aver compiuto 99 anni, ma a parte questo, cercherò di farvi vedere l'altra parte della luna, avendo partecipato a tutti i negoziati fatti a New York che sono stati quelli più complessi e dolorosi.

E dico subito, il testo della Convenzione è un testo di compromesso, di forte compromesso, guadagnato sul campo grazie a un'opera preziosa della presidente della commissione Merbaki e del vicepresidente Eric Sogocio, che è stato preziosissimo negoziatore con tutta la fascia del Sud America, dei paesi dell'America Latina, degli Stati Uniti, dei canadesi, dei giapponesi, di tutto il blocco dei paesi occidentali che ha fatto muro verso un'ipotesi di convenzione larga, che non tenesse conto dei principi del *Serious Crime*, che fosse aperta a qualsiasi tipo di reato commesso.

Dunque, è stato attivato un testo di compromesso che ha delle clausole di salvaguardia conquistate sul campo, le nostre red line che sono state tutte accettate, persino dopo una votazione reiteratamente richiesta proprio dall'Iran, a cui il professor Milanovic faceva cenno. Mi riferisco all'articolo 14, del quale magari poi vi parlerò, sulla pedopornografia. È stata una battaglia dura che aveva, e questo va detto con assoluta chiarezza, un'unica alternativa possibile: il fallimento delle trattative, che si è temuto fino a quattro giorni prima che poi si sbloccasse il negoziato.

Quindi il principio di realtà ci porta tutti a dover dire che bisogna comunque confrontarsi anche con i paesi che non hanno lo stesso modello di democrazie occidentali, bisogna negoziare alla ricerca di quello che non può che essere un testo di compromesso. Bene ha fatto l'ambasciatrice McCarthy a ricordare che l'iniziativa è stata presa da Russia e Cina, sia pure in un contesto geopolitico molto diverso. Bene ha fatto soprattutto a ricordare che si è cercato fin dall'origine di inserire decine e decine di fattispecie criminose che

avevano un unico filo conduttore, quello che portava inizialmente queste norme, ove inserite, alla cooperazione internazionale finalizzata alla repressione del dissenso interno ed esterno a quei paesi, un attentato ai diritti umani e alle democrazie occidentali.

La partita era dunque quella di scegliere un testo di compromesso soddisfacente tra le esigenze di cooperazione giudiziaria, di MLA, di trasferimento di processi e quant'altro di cui si è brillantemente discusso fino ad oggi, con particolare riguardo alla necessità che le prove digitali vengano immediatamente apprese, correttamente conservate e, se mi è consentita una citazione del brillante intervento di Giovanni Salvi, anche a porsi la questione della genuinità della prova acquisita, della correttezza del dato elettronico acquisito, che è fondamento perché nasca un'indagine penale corretta sulla base di dati sperimentati e controllabili, oltre che correttamente conservati, immediatamente bloccati e rapidamente scambiati.

Ma oltre questo, c'era la necessità di creare una barriera per il rispetto dei diritti umani. E quando parlo di diritti umani, mi riferisco a quella elaborazione di dottrina che vede nel cyberspazio non soltanto una frontiera di pericolo criminale, ma uno strumento in più ai circuiti della criminalità organizzata per realizzare i reati più gravi di cui normalmente si occupano le altre convenzioni ONU, dalla Convenzione di Palermo a quella di Merida, come ha ben citato Stefano Mongini. Questo aspetto del diritto umano consentirà forse fra qualche anno di elaborare che, tra i diritti umani fondamentali, rientrerà anche il diritto al libero accesso nel web, al libero accesso nel cyberspazio, la libertà di manifestare le opinioni, che può legittimamente rientrare in una nuova nozione più ampia di diritto umano.

Io mi limito a dire, senza ricordare la fatica che è costato l'inserimento di questa norma, a richiamare l'articolo 2, il comma 2 dell'articolo 6 della Convenzione, che dice proprio che nessuna disposizione della presente Convenzione deve essere interpretata come tale da consentire la soppressione dei diritti umani o delle libertà fondamentali, compresi i diritti connessi alla libertà di espressione, di coscienza, di opinione, di religione, di credo, di riunione pacifica, di associazione, in conformità e in modo coerente con il diritto internazionale applicabile in materia di diritti umani. Chi ha partecipato ai negoziati sa quanto fatica è costato inserire questa norma, insieme all'articolo 24, insieme alle altre norme che sono vere e proprie norme barriera, che consentiranno di impedire la collaborazione allorché vi sia il sospetto che la richiesta di cooperazione giudiziaria si fonda non sulla necessità di perseguire un *Serious Crime*, per come concordato nel testo della Convenzione agli articoli 9 a 16, ma sia fondata sulla necessità di reprimere il dissenso politico interno.

Siamo ben consapevoli di questo, come siamo ben consapevoli che il punto di arrivo del Secondo Protocollo della Convenzione di Budapest è un punto di arrivo a forte trazione occidentale rispetto al quale l'ampliamento che è necessario a livello di Nazioni Unite, dove i paesi potenzialmente sottoscrittori sono 194 (se non sbaglio, il conto è 192, quelli che hanno partecipato direttamente al negoziato), è un punto di compromesso che qualcuno, leggendo le specifiche norme della cooperazione, come ha ben sottolineato per esempio poc'anzi Giovanni Salvi, può leggere in senso minimalista.

Ma la vera partita è garantire uno strumento di cooperazione che, sulla scia di Budapest, possa ampliare la possibilità di cooperazione, unitamente alla necessità di fare *capacity building* per tutti quei paesi che sono ben poco attrezzati nell'azione di contrasto alla criminalità informatica.

Detto questo, volendo riprendere il filo dell'intervento che avevo preparato, sottolineo che la Convenzione affronta necessariamente reati armonizzati, non reati identici. La previsione di una collaborazione in termini di doppia incriminazione è basata sulla fattispecie fattuale perseguita e non soltanto sul titolo di reato. Armonizzare significa non pretendere che in ciascuno stato partecipante ci siano le previsioni criminali identiche o fotocopia, ma è necessario che ci si limiti a descrivere i reati cibernetici sulla base dei *Serious Crimes* così come previsti dalla bozza della convenzione.

Sarà poi lo studio, l'evoluzione, le leggi di ratifica, il percorso cioè successivo alla fase dell'approvazione, che dovrebbe svolgersi a novembre, nei singoli stati membri a spiegare in quale misura questa Convenzione troverà applicazione soltanto per i reati cibernetici in senso stretto, cioè quelli che sono commessi soltanto attraverso il web, oppure se vi è un vincolo di strumentalità con riferimento ai reati cibernetici in senso improprio, cioè a reati ordinari che possono essere commessi anche attraverso l'utilizzo del web. L'esempio classico che si fa è la truffa.

La Convenzione, poi, a me pare apprezzabile in tema di garanzia dell'acquisizione delle prove elettroniche nel processo, quanto mai impegnativo nel contesto del *cloud computing*, contesto in cui i dati sono distribuiti da più fornitori, in più paesi, in più server.

Io credo che il fatto di prevedere, come fa la Convenzione di Budapest, ma in maniera ancora più pregnante rispetto a quest'ultima, la collaborazione dei *server providers* nella fase dell'acquisizione della prova sia una delle parti più interessanti della bozza, che poi dovrà vedere l'attuazione nelle singole leggi degli Stati membri che dovranno recepirle. Da questo punto di vista, l'idea del sistema brasiliano, che ci ha illustrato Eric Do Val Lacerda Sogocio, è sicuramente interessante, va approfondita, va tarata e pensata nell'ambito dei singoli ordinamenti statali.

Del resto, è cruciale coinvolgere il sistema privato in questo ambito. Devo ricordare in proposito che gli stakeholders privati hanno preso parte attiva nei negoziati ONU, erano rappresentati e prendevano la parola. Abbiamo fatto parecchi negoziati e, in questo senso, il mio ricordo va alle varie riunioni informali fatte proprio alla rappresentanza permanente degli Stati Uniti presso le Nazioni Unite, dove spesso si è discusso con l'animo che contraddistingue le migliori democrazie occidentali di aver sempre presente la barra della garanzia dei diritti umani e della libertà delle opinioni, fondamentale per la buona riuscita di questo negoziato che, ripeto, è un testo di compromesso.

Vi sono poi altre norme della Convenzione che certamente creano preoccupazione. La professoressa Severino, nel suo intervento da ex Ministro della Giustizia, ha sottolineato il pericolo che le norme della Convenzione che consentono il trasferimento dei processi e la duplicazione dei processi possano generare, in fase applicativa, incertezze giurisprudenziali. Ma da giurista, da magistrato, mi permetto di dire che dobbiamo fare i conti con un concetto di giurisdizione che la realtà dei fatti ha totalmente scardinato. Chi pensava alla giurisdizione attraverso l'idea superata di un legame col territorio di uno Stato, di un legame con ciò che avviene in uno Stato, di fronte al cybercrime e alle correlate nuove forme di criminalità deve necessariamente fare i conti con un concetto di giurisdizione – una sorta di "quinta dimensione" – che è difficile da catturare, mutuando un'espressione da vecchio pubblico ministero.

L'aspetto che più mi pare interessante è quello di capire come si può operare in questo ambiente diverso, e questo passa proprio attraverso l'assistenza che devono fornire i server provider, senza trincerarsi sul fatto che la legge consente di dislocare i dati in vari server. Quindi, l'idea di Eric, propria del sistema brasiliano, secondo la quale occorre comunque, in ogni paese un rappresentante legale che si assuma la responsabilità di quello che fa il provider, è un'idea che, secondo me, merita di essere approfondita nei prossimi mesi. La dottrina sicuramente darà il suo contributo su questo aspetto.

Credo che sia anche estremamente positivo il risultato raggiunto in termini di obblighi di criminalizzazione anche della pedopornografia in danno dei minori, un passaggio che molti hanno sottovalutato, ma che io qui voglio ricordare, perché vi è una clausola nell'articolo 14 che sanziona la produzione, l'offerta, la vendita, la distribuzione, la diffusione di materiale pedopornografico che riguardi i minori di anni 18.

Il concetto di tutela cui si fa riferimento, è tutto in quel piccolo inciso inserito nella Convenzione, *without right*, "senza diritto". È costato tanta fatica inserire la locuzione *without right.*

I mauritani e gli iraniani, ad esempio, esigevano che la foto a contenuto

sessuale di un minore venisse sempre punita, sempre e comunque, perché contraria alle loro concezioni religiose, anche quando era fatta in piena libertà da un minorenne che aveva piena capacità di compiere atti sessuali e senza alcuna forma di sfruttamento. Vi è stato il voto su questa norma, è una delle pochissime norme su cui l'Iran ha chiesto il voto, e quando ha perso il primo voto ha proposto persino un emendamento in cui si diceva: "Beh, almeno lasciateci il diritto di punire dal punto di vista amministrativo, di sanzionare amministrativamente questo tipo di condotta, perché comunque il minorenne che, sia pure usando la sua libertà, ha rapporti sessuali con un altro partner e si fa pure magari una bella foto, va comunque punito." Ecco, è stata chiesta una votazione anche su questo. Questo dimostra che la bozza della Convenzione delle Nazioni Unite, che io spero venga approvata e magari anche migliorata, presenta un meccanismo di protocolli aggiuntivi sul quale vi è stata battaglia ideologica e politica, perché si diceva: "Ma come, approviamo una convenzione e già prevediamo che ci sia la possibilità di modificarla?"

Bene, questo è stato dovuto a una politica, secondo me, intelligente, della presidente, l'Ambasciatrice Faouzia Boumaiza-Mebarki, la quale, a un certo punto, avendo necessità di chiudere il negoziato, ha dato questa opzione. Questa opzione è sicuramente pensata dai gruppi di paesi che oggettivamente sono risultati sconfitti dall'approvazione di questo testo, con tutti quei firewall, tutti quei muri, tutte quelle barriere che siamo riusciti a inserire, persino sfiorando la pedanteria, perché ad ogni capitolo è stata reintrodotta la norma che riguardava la tutela dei diritti umani. Anche un po' ridondante, l'articolo 6, secondo comma, è stato ripetuto, negli articoli 24 e 35. Abbiamo avuto in ogni settore cura di inserire questo blocco, che servirà ad evitare, io mi auguro, le giustissime preoccupazioni del professor Milanovic in ordine alle – chiamiamole così – democrazie degradate. A me piace, forse con un neologismo, chiamarle *democrature*, cioè una sorta di visione di una specie di dittatura che tutto sommato si trova fondata sul consenso, sia pure un consenso drogato, un consenso costretto.

Però, alla fine, credo che si sia ottenuto un risultato ragionevole, ma che soprattutto, nell'ambito di una trattativa così complessa, si sia ottenuto l'unico risultato tecnicamente possibile, rispettoso delle *red line* delle democrazie occidentali. È un modo per dire che io e tutta la mia delegazione siamo stati molto orgogliosi di offrire la nostra collaborazione per l'affermazione dei limiti delle democrazie occidentali nel rispetto dei diritti umani, in una Convenzione che, devo ricordare, era partita con l'intento della Federazione Russa e della Cina di dotarsi di uno strumento che potesse costringere le democrazie occidentali a collaborare per seguire anche fuori dal loro paese i loro dissidenti. E questo, grazie a Dio, è un rischio che è stato evitato.

IL FUTURO NELLE CONVENZIONI ONU. COOPERAZIONE NELLO SPAZIO VIRTUALE – EFFICACIA DELLE CONVENZIONI ONU E DELLE LEGGI MODELLI NEI CRIMINI INFORMATICI TRANSAZIONALI

Glen Prichard
Capo della Sezione Cybercrime, UNODC

È per me un piacere essere qui oggi e avere l›opportunità di fornire una panoramica della bozza di Convenzione delle Nazioni Unite contro la criminalità informatica, in particolare in relazione al suo intento di fornire un quadro di riferimento per un›efficace cooperazione internazionale nello spazio virtuale.

Questa bozza di Convenzione è il risultato di un processo guidato dagli Stati parte, durato oltre 5 anni e che ha coinvolto 155 nazioni. È stata approvata l'8 agosto di quest'anno dal Comitato ad hoc per l'elaborazione di una Convenzione internazionale globale sul contrasto all'uso delle tecnologie dell'informazione e della comunicazione a fini criminali, incaricato dall'Assemblea generale di elaborare il progetto di convenzione.

Il testo, ancora in bozza, dovrebbe essere esaminato dall'Assemblea Generale entro la fine dell'anno. Una volta adottato ed entrato in vigore, diventerà il primo strumento giuridicamente vincolante sulla criminalità informatica negoziato a livello internazionale e la prima convenzione delle Nazioni Unite sulla giustizia penale in oltre 20 anni.

Il progetto di convenzione è una risposta cruciale degli Stati membri alle sfide che le forze dell'ordine devono affrontare nella lotta contro la criminalità informatica. Queste sfide tecniche e legali non sono nuove.

Da un punto di vista tecnico, lo spazio virtuale è diventato un importante centro per le operazioni criminali, con costi annui previsti a livello globale che raggiungeranno i 10.000 miliardi di dollari entro il 2025. I criminali informatici sfruttano questo spazio virtuale, operando da remoto e in modo anonimo attraverso strumenti come VPN, crittografia e botnet. L'intelligenza artificiale aggrava ulteriormente questi crimini, consentendo truffe sempre più sofisticate e malware più potenti. Le prove risultanti in formato elettronico, sia per i crimini informatici che per altri reati gravi, possono essere disperse in diverse giurisdizioni e sono intrinsecamente vulnerabili alla perdita o alla manipolazione.

A livello legale, le autorità di polizia combattono un crimine che non

conosce confini e possono agire solo all'interno del territorio del proprio Stato. Tuttavia, per le loro indagini e azioni penali, dipendono dall'ottenimento di prove elettroniche che sono disperse tra le varie giurisdizioni e che richiedono misure che possono pregiudicare interessi essenziali degli Stati o che comportano il rischio di abusi, con potenziali violazioni dei diritti umani.

In parole povere, la comunità internazionale ha la responsabilità di sviluppare una soluzione per combattere la proliferazione della criminalità informatica in un paradigma in cui "*i criminali operano alla velocità del denaro e le forze dell'ordine alla velocità della legge*".

Una risposta efficace alla criminalità informatica richiede quindi un quadro di cooperazione internazionale, che bilanci, da un lato, la esigenza di standard comuni e nuovi strumenti procedurali e, dall'altro, garanzie che attenuino i rischi per la sovranità nazionale e altri interessi essenziali.

L'oggetto del mio intervento sarà il modo in cui la bozza di Convenzione delle Nazioni Unite contro la criminalità informatica tenta di raggiungere questo equilibrio, fornendo strumenti per un'applicazione efficace attraverso la cooperazione transfrontaliera e fornendo al contempo garanzie che consentano agli Stati di proteggere i propri interessi nazionali.

Il progetto di Convenzione segue la struttura tipica di uno strumento di giustizia penale internazionale:

- Un capitolo sulla criminalizzazione, in cui gli Stati parte si impegnano a criminalizzare determinate condotte;
- Un capitolo sulle misure procedurali, che aggiorna i mezzi e i metodi di indagine penale a livello nazionale, al fine di indagare e perseguire questi reati;
- Un capitolo sulla cooperazione internazionale, che "internazionalizza" queste misure procedurali per lo scambio di prove e stabilisce meccanismi di cooperazione internazionale per promuovere i procedimenti penali nazionali;
- Inoltre, la Convenzione stabilisce disposizioni sulle misure preventive, l'assistenza tecnica e lo sviluppo di capacità e un meccanismo di revisione per l'attuazione della Convenzione.

Salvaguardie generali per la sovranità

Il progetto di Convenzione prevede esplicitamente il rispetto della sovranità [articolo 4]. Il principio di sovranità si applica anche al cyberspazio, sia nei suoi aspetti interni che esterni. La sovranità interna si riferisce all'autorità sovrana degli Stati sulle infrastrutture informatiche, sugli individui e sulle attività informatiche all'interno del loro territorio. La sovranità esterna si riferisce alla libertà degli Stati di impegnarsi in attività informatiche nelle

loro relazioni internazionali e di stipulare accordi internazionali, compresi quelli sulla criminalità informatica.

Nel contesto di questa Convenzione di giustizia penale, la sovranità viene riaffermata in quanto gli Stati mantengono il loro ruolo di interpreti primari. Essi mantengono la discrezione su come attuare la Convenzione all'interno dei loro sistemi giuridici nazionali e secondo i loro principi giuridici. Inoltre, gli Stati parte applicano il proprio diritto interno nel rispondere alle richieste di assistenza giudiziaria. Infine, poiché le riserve non sono vietate, sono ammissibili a condizione che non siano incompatibili con l'oggetto e lo scopo del trattato.

La sovranità non significa naturalmente libertà dalla legge, ma libertà *all'interno della* legge. Il progetto di convenzione fa parte dell'intero corpus del diritto internazionale ed è regolato e definito dagli obblighi che gli Stati contraenti hanno acconsentito ad assumere nelle loro relazioni internazionali.

Il progetto di convenzione contiene anche riferimenti espliciti ad altri quadri internazionali. Tra questi, il riferimento agli "scopi e principi della Carta delle Nazioni Unite" [PP 1]. Fa inoltre riferimento al "diritto internazionale dei diritti umani" [articoli 6 e 24], affermando l'applicazione delle convenzioni internazionali e regionali sui diritti umani e del diritto internazionale consuetudinario sui diritti umani. Questi riferimenti stabiliscono uno standard minimo esplicito per l'interpretazione e l'attuazione della Convenzione. Inoltre, continuano ad applicarsi altri trattati e obblighi in vigore, come la Convenzione di Budapest.

Giurisdizione

Strettamente correlate alla sovranità sono le regole di giurisdizione, per le quali la criminalità informatica rappresenta una sfida unica, illustrando sia i limiti della sovranità territoriale sia il potenziale di conflitti giurisdizionali tra Stati. Poiché i criminali operano a livello transfrontaliero, le molteplici basi della giurisdizione - territoriale, basata sulla nazionalità o sugli effetti - possono portare a una sovrapposizione di rivendicazioni dell'autorità legale nel perseguire questi reati transnazionali.

La disposizione giurisdizionale del progetto di Convenzione [articolo 22] stabilisce la giurisdizione legislativa degli Stati contraenti. Delinea il potere e la competenza degli Stati parte di assoggettare le persone (o i beni) alle loro leggi e di farle rispettare.

Le basi obbligatorie della giurisdizione si basano sulla territorialità, ossia sul fatto che qualche elemento del reato sia stato commesso nel territorio di uno Stato parte [articolo 22.1(a)] [e le sue varianti, ad esempio la giurisdizione dello Stato di bandiera, articolo 22.1(b)]. Le basi extraterritoriali facol-

tative includono il principio della nazionalità attiva e passiva [articolo 22.2(a-b)] e il principio di protezione, ovvero se un reato è commesso contro uno Stato parte [articolo 22.2(d)].

Consentendo queste diverse basi giurisdizionali, la Convenzione trova un equilibrio tra la possibilità di perseguire efficacemente la criminalità informatica transnazionale e la salvaguardia del diritto sovrano di ciascuno Stato di esercitare l'autorità all'interno dei propri confini e sui propri cittadini. Gli Stati sono inoltre tenuti a consultarsi con le altre parti interessate per ridurre al minimo le sovrapposizioni giurisdizionali improprie quando perseguono i crimini informatici transnazionali [articolo 22.5].

Criminalizzazione

In conformità con questi principi giurisdizionali, il progetto di Convenzione invita gli Stati parte a stabilire 11 reati in conformità con il loro diritto interno [articoli 7-17]. Questi reati vanno dai crimini dipendenti dal cyber, come l'accesso illegale ai sistemi TIC[25] e l'intercettazione illegale di dati elettronici, ai crimini abilitati dal cyber, come i reati relativi all'abuso e allo sfruttamento sessuale dei minori e alla diffusione non consensuale di immagini intime.

Impegnarsi nella criminalizzazione di determinate condotte coinvolge naturalmente la sovranità interna, in quanto implica il potere di definire e promulgare leggi penali. Tuttavia, l'armonizzazione delle leggi penali tra le varie giurisdizioni è essenziale per facilitare la cooperazione internazionale e soddisfare il requisito della doppia incriminazione, che garantisce che uno Stato sia obbligato a prestare assistenza solo nei casi in cui l'atto in questione sia un reato sia nel Paese richiedente che in quello che presta assistenza.

Allo stesso tempo, gli Stati mantengono il diritto di applicare i propri principi giuridici nell'attuazione di queste disposizioni di criminalizzazione. Pur accettando di criminalizzare questi reati, gli Stati mantengono la discrezionalità nel modo in cui inserirli nei rispettivi ordinamenti giuridici nazionali.

Misure procedurali

Le indagini e l'applicazione di questi reati a livello transfrontaliero incontrano difficoltà sia giurisdizionali che tecniche.

Le difficoltà tecniche derivano dalla natura delle prove elettroniche, che sono spesso volatili, disperse tra le varie giurisdizioni e detenute da diver-

25 TIC equivale a "Tecnologie dell'Informazione e della Comunicazione, acronimo italiano dell'equivalente anglofono ICT (NDR).

si fornitori di servizi. Ciò significa che, nella maggior parte dei casi, gli Stati dipendono da entità del settore privato per ottenere le prove necessarie per le loro indagini e per la cooperazione con gli Stati in cui questi fornitori di servizi hanno sede.

Pertanto, la bozza di Convenzione contiene anche nuove misure procedurali per adattare i mezzi e i metodi tradizionali di indagine all'ambiente delle TIC. Queste misure procedurali richiedono agli Stati parte di garantire che, a livello nazionale, le loro autorità siano in grado di conservare [per un massimo di 90 giorni] o ottenere rapidamente dati elettronici attraverso le loro forze dell'ordine o con l'assistenza dei fornitori di servizi.

Queste misure prevedono anche la raccolta in tempo reale dei dati sul traffico e l'intercettazione dei dati sui contenuti, che sono fondamentali per contrastare la criminalità informatica. La raccolta in tempo reale dei dati sul traffico consente alle forze dell'ordine di risalire dalle vittime agli autori dei reati, una capacità essenziale in diversi scenari. Ad esempio, l'identificazione della fonte di un'intrusione nei casi di accesso illegale o il tracciamento della catena di distribuzione di materiale pedopornografico sarebbero quasi impossibili senza questo strumento. Altrettanto importante è l'intercettazione dei dati sul contenuto, che consente alle forze dell'ordine di valutare la natura e la legalità delle comunicazioni. Senza l'intercettazione dei contenuti, spesso è impossibile determinare se una comunicazione è illegale.

Tali misure procedurali possono potenzialmente interferire con i diritti umani, in particolare con il diritto alla privacy e alla libertà di espressione. Per bilanciare queste preoccupazioni, il testo incorpora delle salvaguardie che consentono agli Stati di limitare tali misure. Tali restrizioni possono essere applicate attraverso riserve che specificano alcune categorie o limitando le misure ai reati gravi definiti dal diritto interno di ciascuno Stato. Inoltre, il progetto di convenzione prevede salvaguardie conformi al diritto interno degli Stati parte, nonché il principio di proporzionalità, che è informato dagli obblighi applicabili in materia di diritti umani.

Cooperazione internazionale

I vincoli giurisdizionali nell'applicazione della criminalità informatica derivano dal fatto che la giurisdizione per l'applicazione della legge termina entro i confini di uno Stato, mentre l'applicazione extraterritoriale richiede il consenso dello Stato interessato per le azioni di applicazione extraterritoriali. Pertanto, queste misure procedurali sono "internazionalizzate" attraverso le corrispondenti disposizioni del capitolo sulla cooperazione internazionale, che consentono di estendere questi strumenti investigativi oltre i confini nazionali attraverso richieste di assistenza legale reciproca tra Stati.

Ciò significa, ad esempio, che uno Stato può chiedere a un altro di obbligare un fornitore di servizi locale a intercettare i dati dei contenuti per un'indagine penale. È inoltre previsto che uno Stato possa chiedere a un altro di conservare rapidamente i dati elettronici relativi a un'indagine sulla criminalità informatica, prima di chiedere un accesso formale attraverso le procedure di assistenza legale reciproca.

Inoltre, il progetto di Convenzione [articolo 35.1(c)] prevede anche lo scambio di prove elettroniche per i reati gravi in generale. In altre parole, qualsiasi prova in formato elettronico che possa dimostrare la commissione di un reato grave potrebbe essere condivisa tra gli Stati, rafforzando così in modo sostanziale la cooperazione internazionale in materia penale. Dal momento che oggi praticamente ogni caso penale coinvolge prove elettroniche, questo strumento potrebbe rivoluzionare la cooperazione internazionale in materia di giustizia penale.

Tuttavia, un quadro di così ampia portata sullo scambio di prove ha sollevato anche delle preoccupazioni, che vengono controbilanciate dalla limitazione di questo strumento alla legge sui diritti umani: il progetto di convenzione [articolo 6, paragrafo 2] esenta esplicitamente dal suo campo di applicazione le attività che costituiscono l'esercizio dei diritti umani. Inoltre, le disposizioni sull'assistenza giudiziaria [articolo 40, paragrafi 21 e 22] contengono ampi motivi per rifiutare la cooperazione. Di conseguenza, la cooperazione può essere rifiutata se la richiesta pregiudica la sovranità, la sicurezza, l'ordine pubblico o altri interessi essenziali dello Stato, nonché se l'esecuzione della richiesta è contraria all'ordinamento giuridico dello Stato richiesto. Questi motivi di rifiuto offrono un ampio margine di manovra per le considerazioni sulla sovranità e possono anche includere specifiche preoccupazioni per i diritti umani ed eccezioni di offesa politica, bilanciando così la cooperazione internazionale con la protezione degli interessi nazionali e dei diritti fondamentali.

Infine, una disposizione sulla protezione dei dati personali [articolo 36] consente di rifiutare la cooperazione se lo Stato richiedente non dispone di un quadro equivalente di protezione dei dati o non può garantire l'uso dei dati alle condizioni specificate dallo Stato richiesto.

Per quanto riguarda la fase del procedimento penale e l'esercizio della giurisdizione, il progetto di convenzione [articolo 37] contiene anche una disposizione sull'estradizione. In genere, per l'esercizio della giurisdizione, è richiesta la presenza fisica dell'imputato davanti ai tribunali nazionali [a meno che gli Stati non ricorrano a processi *in contumacia*]. A titolo di salvaguardia, l'estradizione può essere rifiutata se vi sono fondati motivi per ritenere che la richiesta sia stata avanzata allo scopo di perseguire o punire una persona per motivi discriminatori.

Misure preventive e assistenza tecnica

Al fine di fornire un quadro completo contro la criminalità informatica, il progetto di convenzione contiene anche disposizioni sulle misure preventive [articolo 53] e sull'assistenza tecnica [articoli 54-56]. La maggior parte di esse sono facoltative o semi-obbligatorie, e/o da attuare in conformità e nel rispetto del diritto nazionale.

Che differenza fa?

In definitiva, gli strumenti proposti dalla Convenzione hanno il potenziale per rivoluzionare la risposta globale alla criminalità informatica, promuovendo livelli di cooperazione internazionale senza precedenti nel rispetto delle prerogative sovrane.

Essendo aperta a tutti gli Stati al momento dell'adozione, la Convenzione potrebbe migliorare significativamente gli sforzi globali per contrastare la criminalità informatica. Un maggior numero di Stati firmatari significherebbe una maggiore cooperazione internazionale tra le forze dell'ordine e una riduzione dei rifugi sicuri per i criminali.

Inoltre, rivoluzionerebbe la lotta globale contro il crimine in generale, rafforzando la

infine, non rappresenti l'utopia che eliminerà la criminalità informatica, essa costituirà una parte importante degli sforzi continui per combattere la criminalità, sia online che offline, per garantire una libertà uguale per tutti e un ambiente digitale internazionale.

DIBATTITO

Stefano Mogini:

Vorrei anch'io sollecitare e aprire un dibattito, offrendo la possibilità a tutti di intervenire. Naturalmente, la parola va per primo al Procuratore Generale Giovanni Salvi. Prego.

Giovanni Salvi:

La relazione dell'ambasciatrice McCarty tocca esattamente i temi che si volevano mettere in luce, comprese le differenze di approccio; essa è così ampia e approfondita che andrà ben assimilata.

Sarebbe interessante sollecitare il dottor Sogocio a una riflessione sulla efficacia della cooperazione giudiziaria nel quadro della prossima Convenzione ONU rispetto alla Convenzione di Budapest. Ieri si è detto che il draft della nuova Convenzione, in via di approvazione, rappresenterebbe un passo indietro rispetto alla Convenzione di Budapest, perché non consentirebbe un'azione diretta degli Stati in alcuni, pur specifici, ambiti, che è invece possibile nell'ambito della Convenzione di Budapest. Vorrei chieder se condivide questa opinione; in altri termini, si tratta del risultato di una necessità di mediazione, oppure i due approcci sono di fatto sostanzialmente analoghi? E, in ogni caso, ritiene che siano sufficienti per affrontare quello specifico tema che è diverso dalla cooperazione in senso generale sul web. Mi riferisco a quelle specifiche condotte che richiedono un immediato intervento per ricostruire la traccia della provenienza di un attacco, senza dover attendere il consenso dello Stato attaccante.

Eric Do Val Lacerda Sogocio:

La domanda è: in che modo la nuova convenzione si rapporta alla Convenzione di Budapest? E come aiuterà i Paesi ad accedere alle informazioni, richiedere e ricevere i dati necessari per i procedimenti giudiziari?

Il punto cruciale è che ora abbiamo la possibilità di coinvolgere tutti i Paesi in un sistema comune e, dunque, entro un regime unico per la richiesta e la ricezione di informazioni. Va anche sottolineato che fin dall'inizio i Paesi aderenti alla Convenzione di Budapest hanno espressamente dichiarato che la nuova Convenzione deve intendersi come *complementare* a quella di Budapest.

Per i Paesi che già fanno parte della Convenzione di Budapest, ora è

possibile avere uno strumento aggiuntivo da utilizzare. Per i Paesi che non ne fanno parte, invece, la nuova convenzione offre uno strumento che permette loro di collaborare in maniera simile a quella prevista dalla Convenzione di Budapest.

Come ha detto l'ambasciatrice McCarty, il processo della Convenzione ONU potrebbe anche incentivare l'adesione alla Convenzione di Budapest. Noi, come Brasile, abbiamo capito fin dall'inizio che non tutti i Paesi si sarebbero uniti alla Convenzione di Budapest e che sarebbe stato necessario un trattato ONU.

Credo che il valore aggiunto della nuova convenzione sia proprio questo: ora abbiamo un terreno comune, un'armonizzazione delle legislazioni e delle procedure. Questo offre la possibilità di una collaborazione più efficace e tempestiva.

Infine, vorrei evidenziare il tema del capacity building, ovvero dare ai Paesi la possibilità di migliorare i loro sistemi.

Marko Milanovic:

È giusto essere orgogliosi del fatto che i negoziati, cui alcuni dei nostri interventori hanno partecipato, sono giunti alla adozione di un testo finale. Tuttavia, non bisogna presentare il quadro in maniera così rosea. Credo che sia pericoloso presentare la Convenzione come un metodo tecnico e apolitico di collaborazione tra gli Stati su questioni finali quando sappiamo tutti quanto sia facile aggirare il diritto penale per motivi politici.

Io, da avvocato dei diritti umani, penso che ci sia un grande rischio legato alla Convenzione. Per esempio, guardando all'Italia, i magistrati italiani si abitueranno a lavorare con le autorità serbe con pochissime difficoltà, mentre in Serbia, dove la democrazia va degradandosi di anno in anno e il governo perseguita gli oppositori politici, rispondere immediatamente alle richieste di assistenza giudiziaria può significare diventare complici in violazione dei diritti umani e di processi non giusti. Questo è un rischio elevatissimo e non va sottostimato.

Sono d'accordo che bisogna essere vigili. Eric è il tuo punto di vista quando hai detto che il Brasile ha esercitato la sua giurisdizione su X di Elon Musk ma si può applicare la legge di aziende che operano in un territorio perché esse offrono servizi agli utenti ma nell'esempio che ha dato c'è un lato oscuro: c'è stato un giudice che ha deciso di sospendere Twitter e che ha stabilito che ogni cittadino brasiliano che usa il VPN per aggirare il blocco sarà responsabile di un reato. La Cina lo fa, l'India lo fa, è un rischio e un pericolo. Quindi non dobbiamo affrontare questo argomento come una questione di pura collaborazione tecnica; è anche una questione politica e quando si fa la

formazione di giudici, procuratori e funzionari di polizia, essi devono sapere che c'è sempre una dimensione politica.

Marco Roscini:

Domanda per l'ambasciatore Giacomelli. Poiché ha menzionato le contromisure, mi chiedevo se l'Italia avesse una posizione ufficiale sulle cosiddette contromisure collettive, cioè se ritiene che uno Stato che non è vittima di operazioni cybercriminali possa adottare contromisure per aiutare uno Stato che è vittima di quelle operazioni malevole, o se ritiene che solo lo Stato vittima possa reagire. L'Italia nel *position paper* non si esprime sul punto, talché ci si chiede se da allora l'Italia abbia sviluppato una posizione ufficiale sul punto.

Oreste Pollicino:

In questo dibattito vediamo che la dimensione giudiziaria è soltanto una parte di un quadro molto più ampio. Ho ben compreso il Prof. Milanovic quando afferma che questo approccio è simile a quello dell'Iran, ma la presa di posizione brasiliana, a livello della tutela dei diritti umani su Internet, è pionieristica. Quello che io credo che sia molto importante, lo vediamo anche in Europa, è di mettere insieme un'accelerazione giudiziaria che può agire da boomerang con il quadro normativo che dà i principi di certezza anche una buona fede per quanto riguarda il futuro per me è importante abbinare i diversi ingredienti soprattutto per la dimensione brasiliana.

Deborah McCarthy:

Volevo rispondere alle preoccupazioni sollevate riguardo alla possibilità che il processo nella nuova Convenzione possa essere oggetto di abusi. Il prof. Milanovic ha assolutamente ragione. In effetti, abbiamo ottenuto un documento che mira a tutelare la situazione, poiché il livello di fiducia era più basso rispetto alle preoccupazioni iniziali. Abbiamo cercato di inserire quante più tutele possibili. Ad esempio, una proposta del Costa Rica tendeva a permettere di rifiutare l'estradizione per reati politici, ma abbiamo ritenuto che questa potesse creare dei problemi e non è stata approvata. Esistono, infatti, diversi modi in cui i paesi possono rifiutare l'estradizione, anche in presenza di pressioni politiche. Ciò rappresenta una sfida, soprattutto considerando che alcuni paesi potrebbero rifiutare sempre la consegna dei propri cittadini.

C'è anche un altro aspetto che non siamo riusciti a coprire: la protezione di ricercatori di cybersecurity e altri operatori del settore. Come sapete, non esiste una legislazione specifica in merito, tranne in Belgio, mentre negli

Stati Uniti non ci sono leggi in tal senso. Le operazioni in questo campo avvengono tramite modalità differenti e non potevamo introdurre questa protezione attraverso uno strumento internazionale come quello che stiamo creando.

Abbiamo però inserito un capitolo sulla prevenzione. L'articolo 3 prevedeva anche la possibilità di coprire quei soggetti di cui non ci fidiamo, evitando che possano sfuggire alla giustizia semplicemente dichiarando di essere *ricercatori*. Questa è una preoccupazione del settore degli operatori informatici, così come dei giornalisti che potrebbero trovarsi in situazioni di rischio durante i loro viaggi. Purtroppo, esiste ancora un vuoto normativo in questo ambito che bisogna colmare.

Abbiamo inserito nel sistema alcuni elementi per il monitoraggio del processo, ma sono state avanzate delle proposte, soprattutto negli Stati Uniti, per creare un meccanismo di monitoraggio pubblico-privato che coinvolga rappresentanti del settore e dei diritti umani. Questo potrebbe consentire di raccogliere informazioni in modo più rapido rispetto a quanto possiamo fare noi, permettendoci di adottare misure più tempestive. Sebbene il processo non sia perfetto, stiamo considerando la creazione di un gruppo di monitoraggio, un'idea alla quale sarà interessante dare seguito.

Stefano Mogini:

La questione sollevata dal professor Milanovic è certamente molto importante. Mi viene in mente come l'Italia, nella sua giurisdizione, utilizzi le clausole di protezione contro la discriminazione, che sono presenti anche nella convenzione ONU sul Cybercrime, in modo serio e accurato. Credo che questo possa costituire, almeno per il nostro paese, una solida difesa contro gli abusi che potrebbero emergere nelle eventuali richieste di cooperazione giudiziaria basate sulla nuova convenzione, fornendo una difesa efficace.

Eric Do Val Lacerda Sogocio

Il professor Milanovic ha perfettamente ragione. Quando ho scritto questo testo, avevo in mente esattamente questo. Forse è un po' troppo ottimistico e non considera problemi suscettibili che possono sorgere, come le difficoltà politiche che potrebbero emergere. Ricordo di aver sentito da un paese non occidentale riguardo alle tutele dei diritti umani: "Non ci interessa, potete metterci quello che volete, tanto so che i paesi occidentali non collaboreranno comunque con noi." In sostanza, si dicevano certi che, a prescindere dal testo della convenzione, quei paesi occidentali non avrebbero mai collaborato, nemmeno se ci fosse stato un caso molto chiaro e i requisiti fossero stati soddisfatti.

Riguardo alla convenzione, ritengo che siano stati fatti passi avanti importanti. Quando si parla della Corte Suprema brasiliana e di come siano state prese le decisioni, vorrei aggiungere che in Brasile abbiamo lo Stato di diritto e durante i negoziati ho visto che molte istituzioni della società civile cercavano di studiare la Convenzione come uno strumento utile a creare una maggiore istituzionalizzazione nel paese e a promuovere la costruzione dello Stato di diritto. La Convenzione, però, non può fare queste cose; è uno strumento, e credo, in sintonia con quanto detto dall'ambasciatrice McCarthy, che occorra essere vigili. La Convenzione ha previsto degli strumenti per monitorare i vari paesi e fare delle revisioni. Speriamo di includere la società civile in questo processo. Ci sono diversi metodi di controllo previsti dalla Convenzione, ma vale comunque la pena avere una Convenzione. Quando qualcuno dice che forse sarebbe meglio un mondo senza la Convenzione, credo che si sbagli. Con la Convenzione, infatti, abbiamo modi per collaborare, i quali, senza di essa, non sarebbero altrettanto validi.

SPAZIO VIRTUALE: LE SFIDE PER LA COOPERAZIONE GIUDIZIARIA MULTILATERALE, LA CONVENZIONE DI BUDAPEST E LA BOZZA DI CONVENZIONE ONU SUI CRIMINI INFORMATICI

Antonio Balsamo
già Presidente del Tribunale di Palermo - Judge on the Roster of International Judges delle Kosovo Specialist Chambers

Le nuove sfide della criminalità organizzata nello spazio virtuale

"Un mondo enorme, smisurato, inesplorato"[26]: è questa la sensazione che prova Giovanni Falcone a proposito della mafia nel momento in cui Rocco Chinnici gli affida il processo Spatola, il primo processo nel quale sarebbe stata sperimentata una svolta decisiva nella valorizzazione della cooperazione internazionale.

È la stessa sensazione si prova oggi quando ci si confronta con il nuovo volto assunto dalla criminalità organizzata nello spazio virtuale, in quel cyberspazio che ha promosso l›inclusione in tutto il mondo, ha abbattuto le barriere tra paesi, comunità e cittadini, ha reso possibili l›interazione e lo scambio di informazioni e di idee a livello globale, ma, al tempo stesso, ha creato molti fattori di vulnerabilità[27].

Quest'ultima criticità ha una portata sicuramente generale: come evidenziava già nel 2019 l'allora coordinatore antiterrorismo dell'Unione Europea, Gilles De Kerchove, "*the vulnerability of citizens, economies and governments increases proportionally to their connectivity and interdependence*"[28].

Si tratta di una tendenza che è ancora più evidente rispetto alla criminalità informatica transnazionale, oggi caratterizzata da almeno cinque aspetti

26 G. Falcone, *intervista*, in *Rapporto sulla mafia degli anni Ottanta*, a cura di L. Galluzzo - F. La Licata – S. Lodato, Flaccovio editore, Palermo, 1986: «la mafia, vista attraverso il processo Spatola, mi apparve un mondo enorme, smisurato, inesplorato (…) nelle carte del processo Spatola era racchiusa una grande realtà da decifrare. Per venirne a capo, adoperai strumenti che già esistevano ma che pochi avevano sufficientemente utilizzato. Un esempio: ma bastava indagare a Palermo, in Sicilia, in Italia? Se la polizia sequestra qui un carico di stupefacenti destinato agli USA – mi chiesi – perché non andare in USA a studiare gli effetti collaterali di quella operazione riuscita?».

27 Così F. Spiezia, *Minaccia cibernetica e nuovi paradigmi della cooperazione giudiziaria internazionale: Il ruolo di Eurojust*, in *Sistema Penale*, 14 luglio 2023.

28 G. De Kerchove, intervento nel *Justice and Home Affairs (JHA) Council meeting* del 6 e 7 giugno 2019.

innovativi che sono ulteriormente potenziati dall'intelligenza artificiale, e precisamente:

- offensività ad amplissimo raggio
- smaterializzazione
- deterritorializzazione
- velocizzazione
- detemporalizzazione.

Un grande magistrato come Giovanni Salvi, che è riuscito ad ampliare gli orizzonti culturali del mondo della giustizia e ad innovare in profondità gli strumenti di contrasto ai fenomeni criminali transnazionali, ha sottolineato che il *cybercrime* costituisce oggi la sfida più grave, per la sua diffusività in ogni settore e per la minaccia alle infrastrutture vitali della comunità[29].

Da una recente, approfondita ricostruzione compiuta da due dei maggiori esperti di criminalità organizzata[30], emergono tre tendenze evolutive nel modo di operare della realtà mafiosa verificatesi negli ultimi otto anni, che richiedono un corrispondente adeguamento delle strategie di contrasto attraverso l'uso delle tecnologie più moderne.

Il primo fattore di cambiamento ha inizio nel 2016, quando sui *social media* sbarca la «Google Generation Criminale», composta da giovani nati a cavallo tra i due secoli. Con questa presenza sempre più massiccia, le piattaforme social diventano teatri di una strategia di presidio, simile a quella utilizzata nel mondo fisico: esse divengono il motore di un continuo rinnovamento della subcultura mafiosa, che ridefinisce vecchi paradigmi, promuove una sorta di post-verità, e costruisce consenso, senso di identità e di appartenenza, attraverso una predominanza dell'estetica della ricchezza (che ha una speciale valenza attrattiva nei territori della desertificazione scolastica e della disoccupazione imperante) e una idealizzazione del ruolo degli esponenti mafiosi, percepiti come fornitori di protezione e risolutori di problemi per le comunità in cui operano, ovvero come "antieroi" protagonisti della ribellione contro una società che produce diseguaglianza e marginalità.

Il secondo passaggio, manifestatosi con chiarezza dagli anni 2018-2019 in poi, è rappresentato dalla tendenza a veicolare i flussi monetari di alcune delle più potenti organizzazioni criminali di tipo mafioso nei canali informali, attraverso il circuito delle criptovalute, sia per lo svolgimento dei traffici illeciti, sia per le attività di riciclaggio.

---

29 G. Salvi, *Intervento di apertura alla conferenza dei Procuratori generali degli Stati membri del Consiglio d'Europa*, in *Questione Giustizia*, 23/5/2022.

30 N. Gratteri – A. Nicaso, *Il grifone. Come la tecnologia sta cambiando il volto della 'ndrangheta*, Mondadori, 2023.

Infine, la terza tappa, che emerge negli anni 2020-2021 con i primi esiti delle indagini condotte sulle piattaforme Encrochat e Sky ECC, riguarda l'uso dei "criptofonini", forniti a una clientela di varie decine di migliaia di persone da provider che hanno realizzato sistemi estremamente sofisticati di criptazione delle comunicazioni.

Si tratta di soluzioni tecniche finalizzate a neutralizzare tutti gli strumenti investigativi, fino ad allora sperimentati, di captazione delle conversazioni e della messaggistica: sia quelli "tradizionali" (come le intercettazioni telefoniche) sia quelli tecnologicamente avanzati (attuati, ad esempio, con l'installazione di un "captatore informatico", e cioè di un *trojan*, su uno *smartphone*).

I "criptofonini" sono dispositivi nei quali restano disattivate le funzionalità tipiche dei comuni *smartphone*, come i servizi Google, la videocamera, il microfono, il sistema Bluetooth, la porta USB, il sistema di geolocalizzazione. Essi non sono agganciati alla normale rete telefonica o telematica in quanto, per comunicare, si servono di piattaforme informatiche crittografate il cui funzionamento dipende dall'impiego di *server* gestiti da privati ed allocati all'estero. Da qui nasce la necessità di disporre delle chiavi di cifratura, in assenza delle quali i flussi comunicativi scambiati si presentano come sequenze di numeri prive di qualsiasi significato intellegibile[31].

Questi dispositivi, dal costo estremamente elevato, sono stati utilizzati da decine di migliaia di persone, di cui oltre 7.000 in Italia.

Dopo le attività di indagine condotte da squadre investigative comuni costituite dalle autorità francesi, olandesi e belghe con il coordinamento di Eurojust, la relativa messaggistica è stata utilizzata per una serie di procedimenti avviati in Italia, soprattutto in materia di narcotraffico internazionale gestito da esponenti della '*ndrangheta* e di clan stranieri (come quelli albanesi) operanti sul nostro territorio. Il loro impiego probatorio è al centro di una serie di questioni controverse che sono state sottoposte al giudizio di diverse Corti Supreme degli Stati membri[32], compresa la nostra Corte di Cassazione[33], e della Corte di Giustizia dell'Unione Europea[34]: un nuovo e delicatissimo fronte all'interno del già incandescente dibattito sui rapporti tra i mezzi di

---

31 L. Ludovici, *I criptofonini: sistemi informatici criptati e server occulti*, in *Penale Diritto e Procedura, Rivista trimestrale*, 2023, n. 3, p. 417-418.

32 Cfr. il panorama tracciato da S. Ragazzi – F. Spiezia, *Decifrare, acquisire e utilizzare le comunicazioni criptate in uso alla criminalità organizzata: uno sguardo europeo, in attesa del count-down italiano*, in *Sistema Penale*, 26 febbraio 2024.

33 V. le sentenze del 29 febbraio 2024, n. 23755 e n. 23756.

34 V. la sentenza del 30 aprile 2024 della Grande Sezione nel caso M.N., su domanda di pronuncia pregiudiziale proposta dal *Landgericht* di Berlino.

ricerca della prova e le nuove tecnologie[35].

Si sviluppa in questo contesto il "crimine cibernetico organizzato"[36], che potrebbe avvalersi in un prossimo futuro delle potenzialità offerte dall'intelligenza artificiale con conseguenze estremamente allarmanti.

Se queste sono le sfide più recenti poste dalla globalizzazione della criminalità, sul triplice piano della cultura collettiva, della dimensione economica e degli strumenti di comunicazione, non vi è dubbio sulla necessità di un impegno comune che deve coinvolgere tutte le istituzioni, con la stessa apertura mentale che ha contrassegnato l'attività di un grande magistrato capace di cogliere il significato profondo, le radici socio-culturali e le interconnessioni dei fenomeni criminali su cui indagava, come Vittorio Occorsio.

Dalla cooperazione intergovernativa ai nuovi modelli di circolazione transnazionale della prova elettronica

L'impiego della prova elettronica nel procedimento penale copre uno spazio molto più ampio delle ormai tradizionali categorie dei reati informatici in senso stretto (che presuppongono necessariamente processi di automatizzazione di dati e informazioni) e dei reati informatici in senso lato (che concretamente si realizzano con sempre maggiore frequenza attraverso l'utilizzazione della tecnologia informatica, pur senza richiederla necessariamente: già nel 2019, la Commissione Europea ha evidenziato che "per oltre la metà delle indagini penali è necessario accedere a prove elettroniche transfrontaliere", in quanto "le prove elettroniche sono necessarie per circa l'85 % delle indagini penali, e per due terzi di queste indagini vi è la necessità di ottenere tali prove da prestatori di servizi online con sede in un'altra giurisdizione"[37].

Come ha osservato uno dei magistrati italiani con maggiore esperienza internazionale[38], i connotati innovativi della prova elettronica – la sua peculiare localizzazione in più ambienti del mondo digitale, anche sottoposti a diverse giurisdizioni, le fonti private (*Internet Service Provider*), da cui frequentemente origina e presso cui è reperibile, la natura transnazionale del

35 L. Ludovici, *op. cit.*, p. 417.

36 Cfr. A Balsamo – A. Mattarella, *La Convenzione di Palermo a vent'anni dalla sua entrata in vigore: nuove sfide e nuove prospettive*, in *Il diritto penale della globalizzazione*, 2023, n. 2, p. 147 ss.

37 Cfr. la Raccomandazione di Decisione del Consiglio che autorizza l'avvio di negoziati in vista di un accordo tra l'Unione europea e gli Stati Uniti d'America sull'accesso transfrontaliero alle prove elettroniche per la cooperazione giudiziaria in materia penale, COM(2019) 70 final.

38 F. Spiezia, *Minaccia cibernetica e nuovi paradigmi della cooperazione giudiziaria internazionale: il ruolo di Eurojust*, in *Sistema Penale*, 14 luglio 2023.

reato nel cui ambito spesso assume rilevanza, la necessità di strumenti investigativi ad alto tasso tecnologico per la sua acquisizione e per l'intellegibilità dei dati in essa contenuti, la sua volatilità e la sua durata limitata nel tempo, con la conseguente necessità della sua conservazione – sono tutti fattori che riversano il loro carico di novità sui nostri ordinari paradigmi concettuali e normativi, conducendo alla conclusione che siamo in presenza di una seconda rivoluzione copernicana della cooperazione giudiziaria, dopo quella che ha visto il passaggio dalla dimensione intergovernativa ai rapporti diretti tra autorità giudiziarie, con le forme di mutuo riconoscimento.

Da parte della più attenta dottrina[39] è stata proposta una distinzione tra quattro forme di circolazione transnazionale delle prove elettroniche:

a) il modello del "trasferimento probatorio", in cui uno Stato chiede a un altro Stato la trasmissione di elementi probatori di cui l'autorità giudiziaria straniera è già venuta autonomamente in possesso ai fini di un procedimento interno e, quindi, "precostituiti";
b) il modello della "raccolta transnazionale della prova", in cui uno Stato commissiona ad un altro Stato (mediante rogatoria, ordine europeo di indagine, oppure richiedendo la costituzione di una squadra investigativa comune) il compimento di una specifica attività probatoria in relazione ad un procedimento penale in corso;
c) il modello delle "indagini transfrontaliere", tipico della Procura europea (EPPO - *European Public Prosecutor's Office*), in cui la raccolta probatoria oltre i confini dello Stato nel cui territorio è stata avviata l'indagine è affidata a una differente articolazione territoriale del medesimo organismo requirente sovranazionale;
d) il modello previsto dal Regolamento (UE) 2023/1543, relativo agli ordini europei di produzione e agli ordini europei di conservazione di prove elettroniche nei procedimenti penali, che troverà applicazione dal 18 agosto 2026 e configura moduli di circolazione delle "prove elettroniche" che prescindono dai tradizionali meccanismi cooperazione orizzontale e, quindi, da un dialogo fra autorità giudiziarie: infatti, al fine di acquisire i dati conservati in formato elettronico all'estero da un prestatore di servizi operante nell'Unione Europea, le autorità competenti non dovranno più chiedere l'intervento delle autorità giudiziarie dello Stato di esecuzione, ma potranno – sulla base del principio del mutuo riconoscimento, a certe condizioni e se consentito per casi interni analoghi – rivolgersi direttamente al

39 G. Di Paolo, *La circolazione transfrontaliera delle prove elettroniche*, in *Penale Diritto e Procedura,* 2024.

prestatore di servizi straniero, per ingiungergli di produrre (o conservare) dati relativi agli abbonati, al traffico o al contenuto (comprensivi, questi ultimi, di "qualsiasi dato in formato digitale, come testo, voce, video, immagini o suono"), con esclusione delle intercettazioni.

Anche a seguito di quest'ultimo intervento normativo volto ad assicurare un sistema efficiente e globale di acquisizione transfrontaliera della prova elettronica, al fine di agevolarne la circolazione nello spazio giudiziario europeo, si registra comunque la mancanza di una disciplina di armonizzazione delle legislazioni nazionali in ordine alle regole concernenti l'ammissibilità e la utilizzabilità della prova.

Continuano ad esserci, quindi, profonde differenze tra i sistemi processuali degli Stati membri dell'Unione europea, le quali rischiano di compromettere l'efficacia delle nuove forme di cooperazione giudiziaria di fronte, come pure di ostacolare la protezione dei diritti fondamentali delle persone[40].

La recentissima definizione del testo della nuova Convenzione delle Nazioni Unite contro il Cybercrime

La consapevolezza delle difficoltà che l'incessante evoluzione della criminalità informatica crea per l'effettivo esercizio della giurisdizione nazionale di ciascun Paese – un potere tradizionalmente applicato in relazione a fenomeni delittuosi ben definiti nel tempo e nello spazio – sta conducendo la comunità internazionale a progettare nuove forme di cooperazione giudiziaria, che potranno trovare nel prossimo futuro un importante fondamento giuridico nella Convenzione delle Nazioni Unite contro il Cybercrime, il cui testo è stato approvato l'8 agosto 2024 dal Comitato intergovernativo *ad hoc* incaricato delle relative negoziazioni e verrà sottoposto all'Assemblea Generale dell'ONU per la definitiva adozione nel prossimo mese di novembre.

L'approvazione di quella che è destinata a divenire la prima Convenzione ONU sulla criminalità informatica è avvenuta senza opposizione da parte di alcuno Stato, ma è stata accompagnata da forti critiche formulate da un'inedita alleanza tra difensori dei diritti umani e grandi aziende del settore tecnologico.

Va comunque segnalato che anche nell'ambito di una organizzazione internazionale fortemente impegnata nella tutela dei diritti fondamentali, come il Consiglio d'Europa, la nuova Convenzione ONU è stata vista come un risultato politico importante[41]. Lo stesso fatto che l'approvazione del suo

40 G. Di Paolo, *op. cit*.

41 Cfr. *Conventions on cybercrime: The Budapest Convention and the draft UN treaty*, in www.coe.int

testo sia stata realizzata con il metodo del *consensus* (e cioè con una sostanziale unanimità) è particolarmente significativo se si considera che l'avvio del percorso che ha dato vita alla Convenzione era stato contrassegnato da una vistosa divergenza di indirizzo tra la Russia, che aveva formulato la relativa proposta accolta a maggioranza dall'Assemblea Generale dell'ONU nel dicembre 2019, e gli Stati occidentali. In particolare, la Risoluzione 74/247 era stata approvata con 79 voti a favore (tra cui quelli della Russia, della Cina, e della maggior parte dei Paesi del sud-est asiatico), 60 voti contrari (tra i quali quelli degli Stati Uniti, del Regno Unito, del Giappone, dell'Australia e di numerosi Paesi europei), e 33 astenuti.

Nel corso dei successivi lavori, non erano mancate le riserve da parte dell'Unione Europea, del Regno Unito e degli USA, che avevano segnalato l'esigenza di evitare ogni pregiudizio all'applicazione dei vigenti strumenti internazionali, di portata globale o "regionale", che consentono di combattere efficacemente la criminalità informatica, come la Convenzione di Palermo e quella di Budapest, e avevano sottolineato la necessità di includere garanzie appropriate per i diritti fondamentali, compresa la libertà di espressione. Nelle ultime fasi del negoziato, a sua volta, la Russia aveva formulato alcune critiche al testo in via di elaborazione, ritenendolo "sovrasaturo di garanzie dei diritti umani". L'Iran aveva tentato, senza successo, di far rimuovere articoli come quello che consente agli Stati di negare l'assistenza giudiziaria richiesta se ritengono che l'indagine in corso abbia carattere discriminatorio.

La conclusione del percorso negoziale, del quale la Russia ha affermato di essere stata "ispiratrice e leader", è stata salutata con favore anche dagli Stati Uniti d'America, che hanno sottolineato che l'accordo raggiunto "amplia la lotta globale contro il crimine informatico, che è una delle sfide più pervasive del nostro tempo, colpendo le comunità di tutto il mondo", e hanno evidenziato che "la Convenzione fornisce ai paesi ulteriori strumenti per lavorare insieme, anche attraverso la cooperazione nell'attività di contrasto, per affrontare la criminalità informatica, includendo altresì la protezione dei minori". Al tempo stesso, gli Stati Uniti hanno riaffermato che "continueranno a condannare fermamente e a lavorare per combattere le persistenti violazioni dei diritti umani che vediamo in tutto il mondo da parte dei governi che fanno un uso scorretto e abusano delle leggi sulla criminalità informatica e di altre normative e strumenti correlati alla criminalità informatica per prendere di mira difensori dei diritti umani, giornalisti, dissidenti e altri"[42].

Come si è anticipato, vanno però registrate le critiche formulate sia da una serie di ONG impegnate nella difesa dei diritti umani sia dal settore Big

42 Cfr. il comunicato stampa del 9 agosto 2024 del portavoce del Dipartimento di Stato USA.

Tech, che hanno messo in guardia contro uno strumento che potrebbe portare a una "sorveglianza globale".

A ben vedere, i timori legati alla nuova Convenzione possono trovare una efficace risposta soltanto attraverso la decisa valorizzazione del ruolo della giurisdizione, che appare insostituibile per garantire un giusto equilibrio tra tutti i diritti fondamentali coinvolti.

Il quadro giuridico internazionale in via di formazione

Dopo l'adozione della nuova Convenzione ad opera dell'Assemblea Generale dell'ONU, il quadro giuridico internazionale in materia di criminalità informatica transnazionale comprenderà tre strumenti fondamentali:

a) la Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale, adottata a Palermo nel 2000 ed entrata in vigore nel 2003;
b) la Convenzione del Consiglio d'Europa sulla criminalità informatica, adottata a Budapest nel 2001 ed entrata in vigore nel 2004;
c) la Convenzione delle Nazioni Unite contro la criminalità informatica, che dovrebbe essere adottata dall'Assemblea Generale nel novembre 2024 ed entrerà in vigore tre mesi dopo la ratifica da parte di 40 Stati.

La Convenzione di Palermo presenta un carattere autenticamente universale, perché ad essa aderiscono 192 Parti (a fronte di 193 Stati membri delle Nazioni Unite). Si tratta, però, di uno strumento di carattere generale, che ha ad oggetto tutte le forme di criminalità organizzata transnazionale (comprensiva di ogni tipo di realizzazione collettiva di reati gravi – e cioè puniti con pena massima non inferiore a quattro anni – con autori o effetti in una pluralità di Paesi) e non è specificamente mirato sulla criminalità informatica.

La Convenzione di Budapest invece è specificamente dedicata alla criminalità informatica (anche di natura individuale, di ridotta gravità e di dimensione solo nazionale), ma non ha carattere universale: essa rientra tra quelli che, nel linguaggio giuridico delle Nazioni Unite, sono definiti come "strumenti regionali"; è sorta nell'ambito del Consiglio d'Europa ed attualmente aderiscono ad essa 76 Parti, tra cui sono compresi anche diversi Paesi extraeuropei (come l'Argentina, l'Australia, il Brasile, il Canada, il Giappone, il Marocco, la Nigeria, gli Stati Uniti), ma non, ad esempio, la Russia e la Cina.

Anche la nuova Convenzione delle Nazioni Unite contro la criminalità informatica ha specificamente ad oggetto questo fenomeno criminoso, ma si propone di avere una portata universale, colmando così le lacune di tutela dei

beni giuridici inevitabilmente connesse alla limitazione della *membership* (e conseguentemente dell'ambito territoriale di riferimento) della Convenzione di Budapest.

I profili di continuità tra la Convenzione di Budapest e la nuova Convenzione ONU

Un primo confronto tra la Convenzione di Budapest del Consiglio d'Europa e la nuova Convenzione ONU sul cybercrime evidenzia una serie di aspetti di continuità quanto al contenuto delle relative disposizioni.

A) In primo luogo, entrambe le convenzioni prevedono una serie di reati informatici "tipici" che coincide largamente: in particolare, entrambe impongono la criminalizzazione delle condotte di accesso illegale ad un sistema informatico, intercettazione illegale, interferenza con dati elettronici, interferenza con un sistema informatico, abuso di apparecchiature, falsificazione informatica, frode informatica, pornografia infantile. A ciò si aggiungono, per la Convenzione di Budapest, i reati contro la proprietà intellettuale, e, per la nuova Convenzione ONU sul cybercrime, i delitti di furto informatico, *grooming, revenge porn*, riciclaggio.

B) In secondo luogo, entrambe le convenzioni richiedono agli Stati di adottare le misure (legislative e di altra natura) che risultano necessarie per stabilire una serie di poteri e procedure, da applicare obbligatoriamente con riguardo non solo ai reati informatici "tipici", ma anche a tutti gli altri reati commessi attraverso un sistema informatico e alla raccolta di tutte le prove elettroniche dei diversi reati.

Queste misure processuali comprendono:

a) la conservazione rapida di dati elettronici immagazzinati;
b) la conservazione e la parziale divulgazione rapide di dati relativi al traffico;
c) l'ordine di produzione;
d) la perquisizione e il sequestro di dati informatici immagazzinati;
e) la raccolta in tempo reale di dati relativi al traffico;
f) l'intercettazione di dati relativi al contenuto (con riferimento a una serie di gravi reati, da definire nelle legislazioni dei singoli Paesi).

Nella nuova Convenzione ONU alle predette misure (costruite in modo analogo a quelle corrispondenti disciplinate dalla Convenzione di Budapest, anche per quanto attiene alla riservatezza delle operazioni) vengono ad aggiungersi, per i reati informatici "tipici", ulteriori previsioni concernenti il congelamento, il sequestro e la confisca dei proventi del reato, la protezione dei testimoni, l'assistenza e la protezione delle vittime.

C) In terzo luogo, risultano analoghi i principi generali che governano

l'assistenza giudiziaria reciproca, la quale però nella nuova Convenzione ONU – rispetto alla Convenzione di Budapest - presenta un ambito di operatività più circoscritto quanto alla raccolta della prova elettronica (che viene riferita soltanto ai reati gravi, cioè puniti con pena massima non inferiore a quattro anni), ed è caratterizzata da un grado inferiore di vincolatività (traducendosi in un più generico impegno) nei settori della raccolta in tempo reale di dati relativi al traffico e dell'intercettazione di dati relativi al contenuto.

D) In quarto luogo, entrambe le convenzioni prevedono la istituzione di una Rete 24/7 di punti di contatto sempre disponibili per assicurare un'assistenza immediata nell'ambito della cooperazione internazionale, con un'area oggettiva di operatività più estesa nella Convenzione di Budapest ma con un "arsenale di strumenti" più ricco nella nuova Convenzione ONU (la quale fa riferimento anche alla fornitura di dati elettronici per evitare un'emergenza).

Le disposizioni in tema di tutela dei diritti umani contenute nella nuova Convenzione ONU

Nell'ambito della nuova Convenzione ONU sul cybercrime, rimane cruciale la questione della tutela dei diritti fondamentali, che ha formato oggetto di opposte valutazioni (la relativa disciplina, infatti, sarebbe carente secondo le ONG impegnate nella difesa dei diritti umani, e sovradimensionata secondo alcuni Stati, come la Russia e l'Iran).

A ben vedere, vi è una quasi totale sovrapposizione tra le disposizioni dettate dall'art. 15 della Convenzione di Budapest e quelle contenute nell'art. 24 della nuova Convenzione ONU sul cybercrime che disciplina le "condizioni e garanzie" cui devono essere sottoposti – non solo nell'ambito delle indagini condotte a livello nazionale ma anche nel contesto della prestazione della assistenza giudiziaria internazionale richiesta da altri Stati – i poteri e le procedure applicabili con riguardo ai reati informatici "tipici", a tutti gli altri reati commessi attraverso un sistema informatico, e alla raccolta delle prove elettroniche dei vari reati.

Precisamente, con una formulazione analoga al paragrafo 1 dell'art. 15 della Convenzione di Budapest[43], il paragrafo 1 dell'art. 24 della nuova Con-

---

43 Precisamente, il paragrafo 1 dell'art. 15 della Convenzione di Budapest è così formulato: "1. Ogni Parte deve assicurarsi che l'instaurazione, implementazione e applicazione dei poteri e delle procedure previste in questa sezione siano soggette alle condizioni e alle tutele previste dal proprio diritto interno, che deve assicurare un'adeguata tutela dei diritti umani e delle libertà, in particolare dei diritti derivanti da obblighi assunti in base alla Convenzione del Consiglio d'Europa del 1950 per la tutela dei diritti umani e delle libertà fondamentali, alla Convenzione Internazionale delle Nazioni Unite del 1966 sui diritti civili e politici, e agli altri strumenti internazionali applicabili in materia di diritti umani, e che deve considerare il principio di proporzionalità".

venzione ONU sul cybercrime impone a ciascuno Stato di assicurare che l'instaurazione, l'implementazione e l'applicazione dei suddetti poteri e procedure siano soggette alle condizioni e alle garanzie previste dal diritto interno, che deve prevedere la tutela dei diritti umani, in conformità con gli obblighi assunti in base al diritto internazionale dei diritti umani, e che deve incorporare il principio di proporzionalità.

Ovviamente, in considerazione del diverso contesto ordinamentale di riferimento, nell'art. 24 della nuova Convenzione ONU manca un espresso richiamo alla CEDU, presente invece nella Convenzione di Budapest. La CEDU, comunque, rappresenta una delle fonti principali del diritto internazionale dei diritti umani ed è produttiva di precise obbligazioni, per gli Stati che vi aderiscono, anche per quanto attiene alla materia in esame. Non vi è dubbio, quindi, che per tali Stati la eventuale disciplina emanata in attuazione della nuova Convenzione ONU per disciplinare ulteriormente i predetti mezzi di ricerca della prova debba conformarsi alla CEDU.

Questa conclusione è rafforzata dalla considerazione del testo dell'art. 6 della nuova Convenzione ONU, che impegna gli Stati a garantire che l'implementazione delle obbligazioni assunte con tale trattato avvenga in coerenza con gli ulteriori obblighi posti a loro carico dal diritto internazionale dei diritti umani.

Sempre analogamente al disposto del paragrafo 2 dell'art. 15 della Convenzione di Budapest[44], il paragrafo 2 dell'art. 24 della nuova Convenzione ONU stabilisce che, in conformità e ai sensi del diritto interno di ciascuno Stato, le condizioni e garanzie, ove opportuno in considerazione della natura della procedura o del potere in questione, includono anche un controllo giudiziario o altro controllo indipendente, il diritto a un ricorso effettivo, i motivi che giustificano l'applicazione, e la limitazione della portata e della durata di tale potere o procedura. Nella nuova Convenzione ONU viene anzi aggiunto il riferimento al diritto a un ricorso effettivo, non incluso nell'art. 15 della Convenzione di Budapest.

Il paragrafo 5 dello stesso art. 24 specifica che il riferimento al controllo giudiziario o altro controllo indipendente riguarda quanto istituito a livello nazionale. Si tratta, comunque, di una precisazione superflua, non ravvisandosi, allo stato, sistemi preventivi di controllo sovranazionali sui mezzi di ricerca della prova disposti nell'ambito dei procedimenti penali interni ai singoli Stati.

---

44 Il testo del paragrafo 2 dell'art. 15 della Convenzione di Budapest è il seguente: "Quando sia il caso, avuto riguardo alla natura del potere o della procedura, queste condizioni e tutele devono includere, fra l'altro, una supervisione giudiziaria o altra supervisione indipendente, i motivi che giustifichino l'applicazione, e la limitazione dell'ambito di operatività e della durata del potere o procedura".

Infine, per quanto attiene alla tutela dei terzi, il blando contenuto precettivo del paragrafo 3 dell'art. 24 della nuova Convenzione ONU ("Nella misura in cui sia compatibile con l'interesse pubblico, in particolare con l'appropriata amministrazione della giustizia, ciascuno Stato Parte deve considerare l'impatto dei poteri e delle procedure di questo capitolo sui diritti, sulle responsabilità e sugli interessi legittimi dei terzi") è pienamente corrispondente al contenuto dell'art. 15 della Convenzione di Budapest[45].

Una valutazione conclusiva porta quindi a riconoscere che le previsioni dell'art. 24 della nuova Convenzione ONU sul cybercrime non comportano, di per sé, un arretramento nella tutela dei diritti umani rispetto agli standard garantiti dall'art. 15 della Convenzione di Budapest.

Ciò che cambia, piuttosto, è la cerchia degli Stati coinvolti dai due strumenti internazionali: alla maggiore ampiezza della potenziale *membership* della nuova Convenzione ONU, chiaramente, corrisponde una minore omogeneità delle rispettive strutture costituzionali e dei principi ispiratori dei rispettivi ordinamenti giuridici. Ne consegue che disposizioni identiche possono essere applicate in modo profondamente diverso nei vari ordinamenti.

Si tratta di un problema da non sottovalutare, ma che, allo stato, può trovare una graduale soluzione soltanto attraverso due percorsi:

a) da un lato, lo sviluppo di una cultura dei diritti umani comune alle magistrature dei diversi Stati; un obiettivo, questo, che può essere perseguiti valorizzando gli strumenti del "dialogo tra le Corti" e della *cross-fertilization* tra ordinamenti; su questo versante, può giocare un ruolo importante l'attività di assistenza tecnica che trova un significativo spazio nella nuova Convenzione ONU;
b) dall'altro lato, la realizzazione di sistemi di revisione che portino a diffondere le migliori prassi riscontrate in alcuni Paesi, raccomandando le opportune riforme normative e organizzative nei contesti più problematici; un compito, questo, che rientra tra le competenze della Conferenza delle Parti della nuova Convenzione.

Su entrambi questi possibili sviluppi, può assumere un ruolo importante la "diplomazia giuridica" italiana, che nel periodo recente è stata fortemente impegnata nell'assistenza tecnica in favore di altri Paesi e nella implementazione dei meccanismi di revisione delle Convenzioni di Palermo e di Merida, valorizzando le posizioni più moderne del nostro sistema giudiziario.

---

45 Il paragrafo 3 dell'art. 15 della Convenzione di Budapest stabilisce quanto segue: "3. Nella misura in cui ciò sia rispondente all'interesse pubblico e, in particolare, alla buona amministrazione della giustizia, ogni Parte deve considerare l'impatto dei poteri e delle procedure di questa sezione sui diritti, le responsabilità e gli interessi legittimi dei terzi".

Le innovazioni introdotte dal Secondo Protocollo addizionale alla Convenzione di Budapest ed assenti nella nuova Convenzione ONU

Nel testo della nuova Convenzione ONU rimangono assenti alcune importanti innovazioni introdotte dal Secondo Protocollo addizionale alla Convenzione di Budapest, che è stato adottato nel novembre 2021 dal Comitato dei Ministri del Consiglio d'Europa ed entrerà in vigore dopo tre mesi dalla ratifica ad opera di almeno cinque Stati.

Il Secondo Protocollo contiene, in particolare, una articolata disciplina relativa alla protezione dei dati personali e la previsione di procedure volte a rafforzare la cooperazione diretta tra autorità statali ed enti privati, consentendo agli organi investigativi di uno Stato-parte di ottenere informazioni, riguardanti la registrazione di nomi di dominio e gli abbonati, direttamente dagli *Internet Service Provider* aventi sede principale o secondaria nel territorio di un altro Paese[46].

Quest'ultima tipologia di poteri, che richiama da vicino il quarto dei modelli di circolazione transnazionale delle prove elettroniche sopra descritti, non trova riscontro nella nuova Convenzione ONU.

Il valore aggiunto della nuova Convenzione ONU sotto il quadruplice profilo degli organi investigativi comuni, delle misure di contrasto mirate sulla dimensione economica della criminalità informatica, della prescrizione dei reati e degli strumenti extra-penali

Rispetto al complesso delle previsioni contenute nella Convenzione di Budapest e nel suo Secondo Protocollo addizionale, la nuova Convenzione ONU sul cybercrime presenta un importante valore aggiunto, insito nella disciplina dettata dall'art. 48, che richiede agli Stati parte di valutare l'opportunità di concludere accordi o intese bilaterali o multilaterali per la creazione organi investigativi comuni, ad opera delle autorità competenti, in relazione a reati informatici "tipici" costituenti oggetto di indagini, azioni penali o procedimenti giudiziari in uno o più Stati.

Si tratta di una disposizione di contenuto corrispondente all'art. 19 della Convenzione di Palermo, su cui si è costruita una elaborazione di particolare rilevanza innovativa nell'ambito delle Nazioni Unite.

Infatti, la nozione di "organi investigativi comuni" può ricomprendere una pluralità di tipologie, alcune delle quali sono state già diffusamente spe-

46 Il Secondo Protocollo introduce, inoltre, procedure volte a rafforzare la cooperazione internazionale tra le autorità dei diversi Stati ai fini della divulgazione di dati informatici memorizzati, procedure relative all'assistenza giudiziaria di emergenza, disposizioni sulle videoconferenze, sulle squadre investigative comuni e sulle indagini congiunte.

rimentate con importanti risultati – come nel caso delle squadre investigative comuni – mentre altre sono ampiamente da esplorare e possono dare vita a sviluppi ordinamentali di straordinario interesse. Dal coordinamento delle indagini si potrebbe passare alla creazione di un soggetto giuridico ufficiale, dotato di funzioni investigative proprie, complementari con i compiti degli organismi inquirenti dei singoli Stati interessati.

Si tratta, dunque, di una metodologia di organizzazione delle indagini che richiama da vicino il terzo dei modelli di circolazione transnazionale delle prove elettroniche sopra descritti e non trova pieno riscontro neppure nel Secondo Protocollo addizionale alla Convenzione di Budapest, che si limita a dettare disposizioni sulle squadre investigative comuni e sulle indagini congiunte, senza parlare di "organi investigativi comuni".

Al riguardo, deve osservarsi che negli ultimi anni, nell'ambito dei Gruppi di Lavoro della Conferenza delle Parti della Convenzione di Palermo, si è sottolineata la possibilità di tracciare una distinzione tra le semplici "squadre investigative comuni" (*joint investigative teams*), formate per svolgere attività di indagine su specifici casi entro un periodo limitato di tempo, e gli "organi investigativi comuni" (*joint investigative bodies*), contrassegnati da una struttura permanente e competenti per le indagini su determinate tipologie di reato[47].

Proprio la predisposizione di organi investigativi comuni potrebbe essere la strategia più idonea a contrastare gli aspetti più problematici della criminalità informatica transnazionale, in quanto può consentire una significativa velocizzazione della risposta giudiziaria, sganciata da vincoli territoriali e idonea a produrre prove processualmente utilizzabili in una pluralità di ordinamenti, sulla base della applicazione di un *corpus* di garanzie ampiamente condiviso.

Tra le più significative caratteristiche della nuova Convenzione ONU vi è, poi, la forte attenzione al tema della dimensione economica della criminalità informatica, che ha portato all'inserimento di una serie di disposizioni suscettibili di dare un notevole impulso alle relative iniziative giudiziarie, come quelle sulla cooperazione internazionale finalizzata alla confisca e sul connesso recupero dei beni (artt. 49 e 50), sulla cooperazione speciale (art. 51), sulla restituzione e destinazione dei beni confiscati (art. 52).

Un'altra previsione di significativa rilevanza introdotta dalla nuova Convenzione ONU sul cybercrime riguarda il tema della prescrizione. Preci-

---

47 Sul punto v. il *Background paper* preparato dal Segretariato per il *Working Group on International Cooperation* riunitosi a Vienna nei giorni 7-8 luglio 2020 sul tema: *The use and role of joint investigative bodies in combating transnational organized crime*.

samente, l'art. 20 impone agli Stati, sulla base della considerazione della gravità del reato, di stabilire nel proprio diritto interno un lungo termine di prescrizione per l'avvio dei procedimenti per qualsiasi reato informatico "tipico" e di prevedere il prolungamento o la sospensione dei termini di prescrizione qualora il presunto autore del reato abbia eluso l'amministrazione della giustizia.

Si tratta di un preciso impulso alla introduzione di misure normative idonee ad evitare la prescrizione dei reati in questione, che com'è noto sono spesso trattati con tempi processuali suscettibili di far maturare tale causa di estinzione.

Tale previsione è ancora più importante, nel nostro Paese, in quanto la più recente giurisprudenza di legittimità sta orientandosi nel senso di considerare come parametri interposti di costituzionalità, in relazione all'art. 117 Cost., anche le Convenzioni internazionali diverse dalla CEDU ed incidenti sulla materia penale, come la Convenzione di Palermo e quella di Merida[48]. Si tratta di un indirizzo interpretativo suscettibile di essere esteso senz'altro alla nuova Convenzione ONU sul cybercrime.

Infine, va rimarcato come la nuova Convenzione ONU sul cybercrime adotti una strategia ampia di contrasto a tale fenomeno criminale, non limitata agli strumenti penalistici ma estesa alle misure preventive (art. 53), all'assistenza tecnica con la costruzione di capacità (art. 54), allo sviluppo economico (art. 56).

Quali prospettive per il futuro della lotta al cybercrime?

La ormai prossima approvazione della nuova Convenzione ONU non implica affatto una "delegittimazione" degli strumenti finora esistenti.

Al contrario, il quadro giuridico internazionale in via di costruzione può essere imperniato su una utilizzazione congiunta delle tre Convenzioni

48 In questo senso assumono una speciale rilevanza i principi affermati da Cass. Sez. Sez. 5, n. 18837 del 01/02/2024, Rv. 286518, che ha evidenziato che "le Convenzioni delle Nazioni Unite obbligano gli Stati Parte (tra cui l'Italia) a prendere, nella maggiore misura possibile nell'ambito del proprio sistema giuridico interno, le misure necessarie per permettere la confisca dei proventi di reato derivanti dai delitti da esse previsti, tra i quali rientra la corruzione (art. 12 della Convenzione di Palermo e dell'art. 31 della Convenzione di Merida). Ne consegue che l'applicazione della confisca di prevenzione a tutti i diritti aventi natura patrimoniale che scaturiscono da contratti derivati o ottenuti, direttamente o indirettamente, attraverso la commissione di reati di corruzione, costituisce il portato di un obbligo di interpretazione della normativa interna in senso conforme alle norme sulla confisca e sul suo oggetto contenute nelle predette Convenzioni internazionali, sicuramente idonee, per il loro specifico carattere precettivo, ad assumere la valenza di parametri interposti in relazione all'art. 117 Cost.". E' stata così accolta "una interpretazione convenzionalmente conforme del concetto di provento di reato, resa obbligatoria dal disposto dell'art. 117 Cost.".

internazionali, sulle quali è anche possibile impostare una graduale opera di progressiva osmosi normativa, interpretativa e applicativa, con la valorizzazione:

- dei più moderni strumenti e della disciplina sulla tutela dei dati personali contenuta nel Secondo Protocollo addizionale alla Convenzione di Budapest;
- della prospettiva degli organi investigativi comuni tracciata dalla Convenzione di Palermo e dalla nuova Convenzione ONU;
- del ruolo di garante della tutela multilivello dei diritti fondamentali di tutti i soggetti coinvolti, svolto dalla magistratura e dotato di rilevanza essenziale anche per lo sviluppo di quella reciproca fiducia tra i diversi ordinamenti che è indispensabile per il potenziamento della cooperazione giudiziaria internazionale.

Anche nell'ambito del Consiglio d'Europa, viene prospettata con convinzione la possibilità di promuovere una significativa sinergia tra la nuova Convenzione ONU e la Convenzione di Budapest, in particolare attraverso attività di *capacity building* che coinvolgano contemporaneamente il *Cybercrime Programme Office of the Council of Europe* (C-PROC) e l'*United Nations Office on Drugs and Crime* (UNODC) e che potrebbero concretarsi anche nel supporto alla preparazione della legislazione nazionale di vari Paesi, con una particolare attenzione al tema delle garanzie[49].

Nella presente fase storica, emerge con sempre maggiore chiarezza l'importanza di indirizzare la prossima produzione legislativa dell'Unione europea verso due obiettivi ormai ineludibili.

In primo luogo, occorre realizzare una ampia armonizzazione della disciplina delle intercettazioni e di tutti i più moderni mezzi di captazione di comunicazioni, non coperti dal Regolamento (UE) 2023/1543.

Infatti, proprio i più moderni mezzi di ricerca della prova, che sono essenziali per le indagini di mafia, sono rimasti finora al di fuori del processo di armonizzazione normativa, che invece assume una rilevanza fondamentale per adottare in tutti gli Stati (compresa l'Italia) quelle misure, legislative e organizzative, che sono richieste dagli enormi cambiamenti che investono continuamente il mondo delle comunicazioni e che la criminalità organizzata sfrutta continuamente.

In secondo luogo, è indispensabile predisporre una disciplina comune dettagliata sulla responsabilità degli intermediari di internet, con misure specifiche che riguardino tutte i più significativi settori suscettibili di essere usati da organizzazioni criminali (varie forme di messaggistica, social network,

---

49 Cfr. *Conventions on cybercrime: The Budapest Convention and the draft UN treaty*, in www.coe.int

intelligenza artificiale, criptovalute, ecc.), in modo da eliminare le persistenti incertezze sulla portata dei relativi obblighi e delle clausole di non punibilità, dando impulso a una strategia di contrasto moderna e coordinata in questo campo.

L'Europa, se riesce a dare impulso ad una regolamentazione comune in questo delicatissimo ma fondamentale settore, può assumere una posizione di leader nella attuazione della nuova Convenzione ONU sul cybercrime.

DIBATTITO

Carmela Decaro

Faccio parte della Fondazione Vittorio Occorsio in quest'ultima fase di vita, quindi da vera anziana. Però non posso non ringraziare il Ministero degli Affari Esteri e il governo per la straordinaria collaborazione che ha permesso queste due giornate, e non posso esimermi da una riflessione, cui mi ha sollecitata da ultimo il relatore Balsamo, sulla "diplomazia giuridica".

Nello sviluppare questo brevissimo intervento, mi riporto, tra le varie opportunità della mia vita professionale, al periodo nel quale fra il 1997 e il 1999, sono stata a capo del Servizio Rapporti Internazionali e per l'Unione Europea della Camera dei Deputati, e ove ho constatato lo straordinario interesse dell'allora Presidente della Camera, Luciano Violante, per la costruzione di una "diplomazia parlamentare".

Da professoressa di Diritto Costituzionale ho partecipato alla stagione straordinaria del dialogo fra le corti costituzionali che si è aperto tra la fine dello scorso secolo e questo secolo e che ha portato a straordinarie novità, come quella di introdurre nella Costituzione sudafricana il riferimento tra le fonti giuridiche alle sentenze delle corti costituzionali degli altri Paesi.

Oggi sento parlare della possibilità di una diplomazia giuridica e di un dialogo fra le giurisdizioni, che è proprio la lezione delle Nazioni Unite. È una lezione che bisogna tradurre sempre di più in pratica.

Il mio auspicio è che si trovino, come fanno le Camere e le Assemblee parlamentari del mondo e come fa la Corte costituzionale, sempre maggiori occasioni di istituzionalizzazione di appuntamenti, che non sono turistici, ma sono di approfondimento di contenuti e di relazioni umane anche fra le giurisdizioni.

L'Unione Europea, con la Procura Europea, è all'avanguardia, ma nell'ambito di queste attività di monitoraggi, protocolli e forme di revisione, la forza della diplomazia giuridica — come la chiama Antonio Balsamo e che io definirei giurisdizionale — è un canale al quale invito.

Un'ultima sollecitazione. Ho letto proprio qualche giorno fa l'ultimo libro di Mink, che si chiama *Il mondo appiattito*. Bene, una delle soluzioni che egli propone è la giurisdizionalizzazione, l'attenzione al caso singolo, che può portare a un canale di una democrazia del futuro che contrasti l'appiattimento.

Stefano Mogini

Grazie, professoressa. Mi sembra che questo sia veramente un ponte aperto verso nuove riflessioni.

Enzo Bianco

La professoressa Decaro ha anticipato il mio pensiero: dare un plauso all'istituzione che fa da coronamento e suggello a queste intense e quasi concluse due giornate sulla diplomazia giuridica, sulla diplomazia della giurisdizionalizzazione, che io definirei della diplomazia della comunità dei giuristi.

È bellissima la riaffermazione e il monito, che ho sentito chiaramente ieri ed oggi, sulla necessità di prevenire – e, se il caso, evidentemente, reprimere – determinate fattispecie criminali, ma avendo sempre a mente il rispetto delle garanzie e, soprattutto, il rispetto dei diritti umani che ci accomunano.

L'ha detto chiaramente il professor Milanovic, ma l'ha riaffermato, perpetuando un ideale *fil rouge*, il presidente Balsamo questa mattina. Da avvocato – e gli avvocati fanno quello che devono fare, difendere le vittime, ma anche gli accusati e, a volte, i condannati – ribadisco che gli avvocati devono certamente rispettare le sentenze, ma al contempo sempre verificare che siano rispettati i diritti umani.

Ma è necessario che vi sia, come diceva ancora la professoressa, un riconoscimento di tutte le parti in gioco coinvolte, compresa l'avvocatura, che deve essere a fianco, in maniera leale, dell'istituzione.

Io sono favorevole al superamento di sterili sovrapposizioni e contrapposizioni tra attori del sistema e apprezzo molto le parole chiarissime del presidente Balsamo nella riaffermazione di diritti e garanzie che devono vedere anche gli avvocati, come difensori degli ultimi e difensori dei diritti, protagonisti della giurisdizione, insieme agli altri attori del processo e, ancora prima, del procedimento.

Andrea Venegoni

Sono Andrea Venegoni, Procuratore Europeo per l'Italia all'interno di EPPO. Svolgo un brevissimo intervento, posto che la Procura Europea (EPPO) è stata evocata più volte.

Voglio condividere molte delle considerazioni che sono state fatte, anche da Antonio Balsamo. EPPO è un "progetto", se così vogliamo chiamarlo, molto interessante – e lo dico per chi proviene da un contesto "extra Unione Europea" – perché crea all'interno dell'Unione Europea un singolo ufficio e una giurisdizione europea: un ufficio di indagini europeo. Quindi i magistrati

di EPPO non sono più magistrati delle singole giurisdizioni nazionali, ma sono magistrati che operano come magistrati europei.

Nelle indagini di EPPO si pongono molti dei problemi che Antonio Balsamo citava e che, ovviamente, nelle dimensioni sovra-europee si pongono allo stesso modo e forse in maniera ancora più critica, come l'acquisizione della prova, il trasferimento della prova e l'ammissibilità delle prove nei processi che vengono condotti nei singoli Stati.

Però, nello stesso tempo, siccome EPPO ha a che fare con molti reati transnazionali, la competenza di EPPO, pur non focalizzata sul cybercrime, si indirizza su reati che possono anche essere commessi attraverso strumenti informatici, quali, per esempio, il riciclaggio.

L'esperienza di EPPO può ben aprire una strada o comunque essere tenuta presente. Ovviamente non è facilmente replicabile al di fuori dell'Unione Europea, perché EPPO ha potuto essere costituito sulla base di principi comuni agli Stati membri e che li caratterizzano.

Ovviamente, come emerso anche dagli interventi odierni, più si allarga la dimensione degli Stati partecipanti a strumenti o convenzioni, più è difficile trovare una base comune.

Ma, nello stesso tempo, siccome EPPO si muove all'interno di un quadro giuridico e normativo dell'Unione Europea ed anche extraeuropeo che è in continua evoluzione – e penso, per esempio, alle possibili estensioni della competenza di EPPO anche a reati transnazionali che vanno al di là dell'attuale competenza – noi ci sentiamo parte di questo processo.

Credo che la base per lo sviluppo di questi strumenti sia sempre una volontà politica importante; una volontà politica che gli Stati dell'Unione Europea hanno raggiunto quando si è trattato di costituire EPPO, e che è ugualmente necessaria quando si tratta di gettare le basi per strumenti di contrasto transnazionale di dimensione ancora più elevata. E appunto, più si allarga la platea dei partecipanti, più è difficile approdare a una volontà politica chiara e specifica.

Ma se, in qualche modo, l'esperienza di EPPO potesse essere utile per lo sviluppo di ulteriori strumenti o di ulteriori mezzi di contrasto alla criminalità organizzata transnazionale, EPPO è sicuramente a disposizione e ci farebbe piacere che venisse tenuto presente.

TAVOLA ROTONDA

L'EFFICACIA DELLA COOPERAZIONE MULTILATERALE DI POLIZIA E GIUDIZIARIA NEL CYBERSPAZIO – ESPERIENZE IN MATERIA

Eugenio Albamonte
Sostituto Procuratore della Repubblica – Roma

Prima di iniziare a entrare nell'argomento, anch'io voglio ringraziare la Fondazione Occorsio e in particolare Eugenio e Vittorio Occorsio e Giovanni Salvi, che presiede il comitato scientifico della Fondazione. Ringrazio la Fondazione innanzitutto perché esiste e, in secondo luogo, perché, a fianco di un'attività di impegno civile nella memoria proattiva di un periodo drammatico per la storia del Paese, che è quello della violenza terroristica e dell'utilizzazione della forza bruta per affermare la propria visione politica, si impegna in tanti campi. In particolare, in questo campo, a me è particolarmente caro; la ringrazio anche per avermi voluto coinvolgere con un piccolo contributo in questa giornata di un convegno così importante e strategico.

L'efficacia della cooperazione multilaterale di polizia e giudiziaria nello spazio e le esperienze in materia sono il focus del nostro incontro. La nostra tavola rotonda può essere soprattutto un confronto di esperienze. Divideremo il nostro tempo in due brevi comunicazioni per i miei relatori: una un po' più lunga, di una decina di minuti, e una inevitabilmente più breve, in cui vorremo, in un primo giro, fare il punto, dai diversi punti di vista, dello stato dell'arte, cioè di come si è evoluta la cooperazione giudiziaria, soprattutto in questo campo. Premetto che, in pochi anni, si sono fatti passi da gigante. Però restano anche dei punti critici che oggi viviamo. In un secondo giro, invece, affronteremo qualche spunto su possibili forme di implementazione e rafforzamento della cooperazione giudiziaria.

Mi occupo da circa 15 anni, presso la Procura di Roma, di cybercrime e inevitabilmente, quindi, di indagini nel cyberspazio. Un tipo di indagini che sono intimamente e indissolubilmente collegate alla cooperazione giudiziaria, che siano le forme più semplici di cooperazione o le forme più complesse. Si tratta, ad esempio, di acquisire un dato di traffico da un *internet service provider* esterno o, all'opposto, nei casi più estremi, più gravi, più complicati, di individuare l'operatività di complesse strutture informatiche operanti in diversi Paesi, che hanno funzioni criminali. Funzioni che noi definiamo spes-

so criminali soltanto perché, come si è detto in più passaggi in queste giornate, non siamo sicuri dell'attribuzione, o meglio non possiamo con certezza attribuire spesso a queste azioni la veste criminale, ma la natura di veri e propri atti ostili provenienti da strutture statuali straniere, rispetto a circostanze rispetto alle quali spesso abbiamo elementi di concreto e grave sospetto. Ma, appunto, il tema dell'attribuzione mantiene queste condotte nel contesto dei fenomeni criminali. La necessità della cooperazione emerge chiaramente dalla struttura degli attacchi informatici. Questi, infatti, non mettono in correlazione diretta l'infrastruttura critica attaccata con quella attaccante, ma spesso utilizzano una serie di infrastrutture "proxy", cioè di collegamento e di offuscamento, collegate in varie parti del mondo.

In questi 15 anni si è passati da una cooperazione inizialmente assai farraginosa, burocratica, passiva, con tempi di attesa quasi biblici, a una cooperazione sempre più operativa e performante, fino a raggiungere oggi, con gli strumenti a disposizione, un livello di eccellenza. Questo è avvenuto grazie all'evoluzione degli strumenti di cooperazione e quindi all'introduzione delle squadre investigative comuni, degli ordini di indagine europei, e al rafforzamento delle competenze di Eurojust ed Europol, rappresentati in questa tavola rotonda rispettivamente dal collega Hannes Glantshnig (Eurojust) e da Edvardas Sileris (Europol).

Un altro elemento determinante è stata la diffusa e crescente consapevolezza, all'interno dei vari sistemi e stati, dell'importanza e della gravità della minaccia cibernetica.

Non possiamo però nasconderci dietro un dito: ciò che realmente rafforza la cooperazione è il cosiddetto "nemico comune". In questa fase storica, tutti i Paesi europei e molti Paesi non europei, ma appartenenti comunque all'area culturale delle democrazie occidentali, sono sottoposti ad attacchi informatici che hanno prevalentemente lo stesso movente, la stessa matrice e la stessa provenienza. È evidente che queste dinamiche rafforzano l'operatività della cooperazione.

Ciascuno di noi, paesi attaccati, sa che una prova rinvenuta attraverso l'analisi di un server attaccato, o una traccia informatica, da sola non porta a nulla. Tuttavia, messa insieme a un altro elemento, magari trovato in una scena del crimine informatico olandese, canadese o statunitense, può contribuire a dare un quadro più ampio e consentire una migliore capacità di individuazione dell'insidia.

Oggi, quindi, assistiamo a una cooperazione che si muove quasi come quella tra uffici giudiziari dello stesso paese, con incontri molto serrati, la cui funzione non è soltanto di scambio formale di informazioni, ma altresì di condivisione di strategie e di programmazione di azioni investigative. Abbia-

mo squadre di polizia giudiziaria che, con il supporto della polizia dello Stato locale, operano direttamente affiancando la polizia dello Stato locale in teatri diversi dal proprio nazionale. Quindi, polizie giudiziarie che si muovono per accedere all'attività investigativa insieme alla polizia nazionale sul territorio straniero.

Ciò ovviamente determina anche un beneficio di portata più generale: in primo luogo per l'acquisizione della prova secondo modalità che siano più coerenti con i sistemi ordinamentali dei vari stati; in secondo luogo, per la condivisione delle prassi investigative sul campo; in terzo luogo, per la condivisione delle tecnicalità, delle strutture e dei mezzi, elementi questi ultimi che nel contesto sono tanto importanti quanto le tecniche. Quindi, la diffusione di programmi che ciascuna polizia giudiziaria porta con sé e che vengono utilizzati congiuntamente su un teatro del crimine determina una maggior circolarità anche delle tecnicalità sottostanti.

E tuttavia, nonostante i passi in avanti fatti dalla cooperazione in questi anni, non riusciamo ancora a raggiungere risultati ottimali. Questo è il tema che vorrei consegnare ai miei interlocutori, ai quali chiedo in primo luogo di fare il punto, insieme e ciascuno dai diversi punti di osservazione, circa lo stato dell'arte e le criticità che, nonostante le positività derivanti da potenziati strumenti di cooperazione, impediscono di raggiungere ancora risultati adeguati.

Ivano Gabrielli

Direttore della Polizia Postale e delle Telecomunicazioni

Soltanto un paio di ringraziamenti per la straordinaria opportunità di vivere queste due giornate eccezionali di dibattito, tanto per il livello delle interlocuzioni, quanto per gli spunti che porterò con me, calandoli nell'attività operativa che mi vede dirigere la struttura della Polizia Postale e delle Telecomunicazioni.

L'ex Ministro dell'Interno Enzo Bianco ha prima accennato a quella visione politica che ha portato l'Italia già nel 1999-2000 a ritenere necessario che vi fosse, all'interno della Polizia di Stato, un corpo specializzato nel Cybercrime. Saluto al riguardo il Prefetto Pansa, che è stato il primo interprete di tale disegno, disegno che ci portava ad essere tra i più risalenti corpi di polizia che si occupano di Cybercrime.

Rimango nei confini del tema affidatomi, quello della cooperazione internazionale di polizia. Deve essere cooperazione giudiziaria, il rovescio della medaglia di quello che così faticosamente si è costruito attorno alla Convenzione ONU sul Cybercrime. Ho seguito sin dall'inizio i lavori, conosco le difficoltà affrontate e anche le diffidenze iniziali delle varie rappresentanze rispetto a una proposta di convenzione che veniva da un mondo così diverso da quello dei cosiddetti paesi "LDCs"[50]. Colgo l'importanza straordinaria del risultato di aver costruito un terreno comune per quanto riguarda l'individuazione dei crimini informatici.

Appare straordinario il riferimento fatto prima allo spostamento della discussione dalla sicurezza informatica tout court alla criminalità informatica, terreno comune dove dialogo e cooperazione trovano spazio fertile. Qui si rende effettiva la tutela che alcuni diritti devono avere, anche a livello internazionale. È un fenomeno criminale che muove 10,5 trilioni di dollari di profitti nel mondo e nel quale oggi oltre il 90% delle attività investigative dipende da forme di cooperazione internazionale.

Tali attività investigative possono assumere varie forme, come descritte in modo puntuale dal Presidente Balsamo. Vi è la cooperazione "statica", come lo scambio di informazioni sostenuto dalla Convenzione di Budapest con la rete dei punti di contatto, che ha permesso di approdare al congelamento di fonti di prova distanti nel mondo, ma anche, oggi sempre di più, la cooperazione "dinamica", alimentata da investigazioni comuni, che vivono all'interno di organismi di cooperazione e che si avvalgono spesso di squadre investigative comuni.

---

50 Acronimo anglofono equivalente a *Least Developed Countries*, ovvero Paesi meno sviluppati (NDR).

La cooperazione richiede sempre più un'effettiva collaborazione operativa, attraverso attività congiunte, e ciò perché le forme di criminalità, soprattutto quelle più gravi, come la pedopornografia e le frodi informatiche su scala internazionale, hanno una dimensione così radicalmente transnazionale che le indagini non possono che condividersi tra più Stati. Ciò permette alla comunità internazionale di avvantaggiarsi nel perseguimento e nell'individuazione dei responsabili di crimini di ampia portata.

La dimensione internazionale è intrinseca al Cybercrime. Molto si è fatto in termini di cooperazione internazionale, specialmente in Europa, con strumenti come i Joint Investigation Teams e l'Ordine europeo di indagine, che ci permettono oggi di parlare di indagini condivise, sia a livello di polizia che di magistratura, grazie al coordinamento di Eurojust.

Questo è il terreno su cui deve muoversi l'evoluzione internazionale del contrasto al Cybercrime, anche a livello extraeuropeo: la creazione di un framework legale comune per i mezzi di ricerca delle prove, la qualificazione dei reati, l'acquisizione, lo scambio e la validazione delle prove, sulla base di una visione comune degli strumenti e delle attività investigative concrete. Ciò richiede la nascita e l'evoluzione di organismi di cooperazione internazionale e di forze di polizia specializzate che possano operare fianco a fianco, validando l'attività investigativa nel contrasto a fenomeni di natura transnazionale.

Questo è il futuro verso cui muoversi. La Convenzione ONU sul Cybercrime rappresenta il punto di partenza, il framework che si aspettava da tempo; essa consentirà di essere non solo più efficaci, ma anche più efficienti, favorendo economie di scala e la nascita di gruppi investigativi che si avvantaggino di una cultura giuridica comune.

Hannes Glantshnig
Vice Presidente del Team Cybercrime, Eurojust

Introduzione: La crescente minaccia della criminalità informatica

La criminalità informatica non è un fenomeno nuovo, ma la sua portata, le sue dimensioni e la sua sofisticazione sono cresciute in modo esponenziale negli ultimi anni. La rivoluzione digitale ha creato opportunità senza precedenti per il progresso, l'innovazione e la connettività. Tuttavia, ha anche aperto nuove frontiere per le attività criminali che trascendono i confini nazionali, sfruttano i progressi tecnologici e sfidano le fondamenta stesse dei nostri quadri giuridici e istituzionali. Queste sfide vanno dall'enorme volume di dati nelle indagini al crescente uso dell'anonimizzazione e della crittografia da parte dei criminali. Ognuna di queste sfide pone ostacoli significativi alle forze dell'ordine e alla magistratura e per affrontarle sono necessarie soluzioni innovative e una maggiore cooperazione internazionale.

Volume e complessità dei dati

Una delle questioni più urgenti evidenziate è l'enorme volume di dati coinvolti nelle indagini sulla criminalità informatica. Oggi abbiamo a che fare con indagini che richiedono l'analisi di terabyte o addirittura petabyte di dati. L'archiviazione, la gestione e l'analisi di tali enormi quantità di informazioni richiedono strumenti tecnologici avanzati, risorse significative e, soprattutto, la capacità di cooperare senza soluzione di continuità tra le varie giurisdizioni.

La gestione di grandi volumi di dati non è solo una sfida tecnica, ma anche giuridica. Dobbiamo garantire che i dati siano raccolti, archiviati e analizzati in modo da rispettare la privacy e i diritti umani, consentendo al contempo indagini penali efficaci. Questo delicato equilibrio è difficile da raggiungere, soprattutto quando i quadri giuridici variano notevolmente da una giurisdizione all'altra.

La frammentazione delle leggi sulla conservazione dei dati in Europa, aggravata dall'invalidazione della Direttiva sulla conservazione dei dati da parte della Corte di Giustizia dell'Unione Europea, ha creato un mosaico di normative che spesso portano alla perdita di dati cruciali prima che possano essere accessibili alle forze dell'ordine.

Anonimizzazione e crittografia: L'arma a doppio taglio

L'anonimizzazione e la crittografia sono strumenti fondamentali per la protezione della privacy e la sicurezza delle comunicazioni nell'era digitale. Tuttavia, questi stessi strumenti sono sempre più utilizzati dai criminali per

nascondere le loro attività, rendendo straordinariamente difficile per le forze dell'ordine rintracciare e perseguire i criminali informatici. Le diverse disposizioni di legge degli Stati membri dell'UE in materia di accesso alle informazioni criptate aggiungono un ulteriore livello di complessità ai nostri sforzi.

Per esempio, mentre alcuni Paesi hanno leggi che obbligano a decifrare le informazioni in determinate condizioni, altri hanno forti protezioni contro tali azioni. Questa disparità legale non solo complica le indagini, ma crea anche paradisi sicuri per i criminali informatici che possono operare impunemente in giurisdizioni con leggi meno severe.

Operazione Trojan Shield

Nel giugno 2021, l'Operazione Trojan Shield è stata un'operazione di contrasto internazionale coordinata e su larga scala condotta dall'FBI in collaborazione con Eurojust, Europol e diverse altre agenzie di contrasto in tutto il mondo. L'operazione ha preso di mira le reti globali del crimine organizzato sfruttando la fiducia dei criminali in una piattaforma di comunicazione criptata nota come ANOM.

ANOM era un'applicazione di messaggistica sicura sviluppata e controllata segretamente dall'FBI. L'applicazione era stata progettata per imitare altri servizi di messaggistica criptata frequentemente utilizzati dai criminali, ma aveva una differenza fondamentale: permetteva alle forze dell'ordine di monitorare tutte le comunicazioni in tempo reale. La piattaforma è stata distribuita alle reti criminali attraverso agenti e informatori sotto copertura, guadagnando credibilità tra le organizzazioni criminali di alto livello coinvolte nel traffico di droga, nel riciclaggio di denaro e in altre attività illecite.

In tre anni sono stati intercettati più di 27 milioni di messaggi da 12.000 dispositivi in oltre 100 Paesi. Questi messaggi hanno fornito informazioni preziose sulle operazioni criminali, tra cui spedizioni di droga pianificate, attività di riciclaggio di denaro e aggressioni violente. I dati raccolti da ANOM hanno permesso alle forze dell'ordine di effettuare numerosi raid e arresti in tutto il mondo.

L'operazione ha portato all'arresto di oltre 800 persone in tutto il mondo, al sequestro di oltre 8 tonnellate di cocaina, 22 tonnellate di cannabis, 2 tonnellate di droghe sintetiche, 250 armi da fuoco, 55 veicoli di lusso e oltre 48 milioni di dollari in contanti e criptovalute. Queste azioni hanno inferto un colpo significativo alla criminalità organizzata, interrompendo diverse imprese e reti criminali.

L'operazione Trojan Shield ha dimostrato la potenza della collaborazione internazionale e delle strategie innovative di applicazione della legge

nell'affrontare le complessità del crimine organizzato moderno. Utilizzando una piattaforma segreta, le forze dell'ordine hanno dimostrato che sfruttando la tecnologia è possibile infiltrarsi e smantellare efficacemente le reti criminali che operano a livello transfrontaliero.

Questa operazione è un esempio di come una cooperazione fluida e veloce tra le forze dell'ordine di tutto il mondo, unita a tattiche tecnologiche avanzate, possa avere un impatto significativo sulla criminalità globale.

Cooperazione internazionale: Una necessità, non una scelta

La natura transnazionale della criminalità informatica rende la cooperazione internazionale non solo auspicabile, ma essenziale. Tuttavia, realizzare una cooperazione efficace è più facile a dirsi che a farsi. Le barriere legali e logistiche spesso ostacolano il flusso di informazioni e prove tra i Paesi, rallentando le indagini e permettendo ai criminali di sfruttare le lacune giurisdizionali.

Il progetto SIRIUS di Eurojust ed Europol, che promuove la cooperazione nelle indagini sui reati gravi, è un ottimo esempio di come la collaborazione internazionale possa essere efficace. Grazie ad ampi programmi di formazione, alla condivisione delle migliori pratiche e alla stesura di relazioni esaustive, il progetto ha fatto passi da gigante nel miglioramento della cooperazione transfrontaliera. Tuttavia, questi sforzi devono essere sostenuti da quadri legislativi solidi e armonizzati che facilitino, anziché ostacolare, la cooperazione internazionale.

L'introduzione di nuovi strumenti legislativi dell'UE, come il Pacchetto e-evidenza e la Legge sui servizi digitali, rappresenta un progresso significativo. Questi quadri mirano a snellire i processi e a migliorare la capacità delle autorità competenti di gestire grandi insiemi di dati, applicare le normative e promuovere la cooperazione internazionale. Tuttavia, la vera misura della loro efficacia sarà nella loro applicazione pratica e nella misura in cui potranno essere integrati nelle strategie esistenti negli Stati membri e oltre.

Intelligenza artificiale: La prossima frontiera

Guardando al futuro, la regolamentazione dell'intelligenza artificiale (IA) a livello globale sarà fondamentale. L'IA ha un immenso potenziale sia per combattere che per facilitare la criminalità informatica, il che la rende un'arma a doppio taglio. che richiede una gestione attenta. La legge sull'intelligenza artificiale dell'Unione Europea è un passo lodevole nella giusta direzione, con l'obiettivo di creare un quadro normativo solido che affronti le implicazioni etiche e di sicurezza dell'IA. Tuttavia, l'IA non è limitata dai

confini nazionali e la sua regolamentazione richiederà uno sforzo concertato a livello globale.

L'integrazione dell'IA nelle attività dei criminali informatici aggiunge un ulteriore livello di complessità a un panorama già difficile. L'IA può essere utilizzata per automatizzare e scalare gli attacchi informatici, rendendoli più efficienti e difficili da rilevare. Ad esempio, il malware guidato dall'intelligenza artificiale può imparare dall'ambiente circostante e adattare il proprio comportamento per evitare il rilevamento da parte delle misure di sicurezza tradizionali. Ciò rende urgente la necessità di nuove strategie e strumenti per combattere la criminalità informatica potenziata dall'intelligenza artificiale.

Allo stesso tempo, l'IA può essere un potente strumento per le forze dell'ordine. Gli algoritmi avanzati di IA possono setacciare vaste quantità di dati per identificare modelli, prevedere comportamenti criminali e persino simulare i potenziali risultati di diverse strategie di applicazione della legge. Tuttavia, l'uso dell'IA nelle forze dell'ordine solleva anche importanti questioni etiche e legali. Come possiamo garantire che i sistemi di IA siano trasparenti, responsabili e privi di pregiudizi? Come bilanciare l'esigenza di sicurezza con la tutela dei diritti individuali?

L'inquietante ascesa del materiale generato dall'IA sugli abusi sessuali sui minori

Un altro sviluppo molto preoccupante nel campo della criminalità informatica è il crescente uso dell'intelligenza artificiale (IA) per creare materiale pedopornografico (CSAM). Negli ultimi anni abbiamo assistito a un aumento vertiginoso sia della quantità che della qualità del CSAM generato dall'IA, ponendo sfide senza precedenti alle forze dell'ordine, alla magistratura e alla società in generale.

L'intelligenza artificiale è in grado di generare immagini e video altamente realistici di abusi su minori, confondendo i confini tra contenuti reali e contenuti inventati. Ciò crea notevoli difficoltà per gli investigatori che devono distinguere tra casi di abuso reali e materiale generato dall'IA. Il processo di verifica dell'autenticità di questi contenuti non solo richiede tempo, ma è anche mentalmente ed emotivamente faticoso per le persone coinvolte nelle indagini. Inoltre, l'esistenza di materiale falso così realistico complica i processi legali, portando potenzialmente a problemi nell'azione penale e nella giustizia per le vittime.

Tuttavia, i danni causati dal CSAM generato dall'intelligenza artificiale si estendono ben oltre l'ambito digitale. I perpetratori spesso usano immagini di bambini reali - a volte bambini nelle loro stesse vicinanze - come base per questi materiali generati dall'IA. Ciò non solo mette a rischio direttamente

questi bambini, ma perpetua anche un ciclo di abusi, in cui il consumo di questo materiale alimenta la domanda di contenuti più estremi ed espliciti. L'esistenza stessa di CSAM generato dall'IA può incoraggiare gli autori a commettere ulteriori reati, tra cui l'adescamento e il rapimento delle vittime.

La situazione è aggravata dall'emergere di chatbot maligni guidati dall'intelligenza artificiale che inducono attivamente i sospetti a commettere reati. Questi chatbot possono coinvolgere i potenziali criminali con contenuti espliciti, tra cui immagini e messaggi vocali, e persino fornire guide dettagliate sull'adescamento, il rapimento delle vittime e l'elusione del rilevamento. Questi strumenti di intelligenza artificiale sono progettati per sfruttare le vulnerabilità degli individui, spingendoli ulteriormente sulla strada del comportamento criminale e rendendoli più pericolosi per la società.

L'ascesa del CSAM generato dall'IA e l'uso di chatbot maligni guidati dall'IA rappresentano una nuova e terrificante frontiera della criminalità informatica. Evidenziano la necessità di una risposta sfaccettata che includa soluzioni tecnologiche, quadri giuridici solidi e una maggiore cooperazione internazionale. Le forze dell'ordine devono essere dotate dei più recenti strumenti di rilevamento dell'IA e devono essere formate per affrontare queste nuove forme di criminalità. Allo stesso tempo, devono essere introdotte norme più severe che regolino lo sviluppo e l'uso delle tecnologie dell'IA, per evitare che vengano sfruttate da elementi criminali.

Non si tratta solo di una sfida per le forze dell'ordine, ma di un imperativo morale per l'intera società. Lo sfruttamento dei bambini, sia attraverso materiali generati dall'IA che con altri mezzi, è uno dei crimini più odiosi che si possano immaginare. Dobbiamo lavorare insieme, al di là dei confini e delle discipline, per proteggere i membri più vulnerabili della nostra società dai pericoli posti da queste tecnologie emergenti.

Esempio di utilizzo dell'IA da parte delle forze dell'ordine

Per illustrare il potenziale delle tecniche avanzate di IA nelle moderne attività di contrasto, si consideri l'approccio adottato da un Paese europeo nell'affrontare l'odioso crimine del materiale pedopornografico (CSAM) che circola online. Le forze dell'ordine di questo Paese hanno integrato la tecnologia di riconoscimento vocale per identificare i sospetti che parlano nella lingua nazionale all'interno dei video illeciti.

Questo approccio innovativo inizia con la raccolta di CSAM da varie piattaforme online. I contenuti vengono poi elaborati utilizzando sofisticati algoritmi di intelligenza artificiale in grado di riconoscere le diverse lingue.

Ma il processo non si ferma qui. Il video viene ulteriormente analizzato utilizzando una tecnologia di riconoscimento facciale guidata dall'intelligen-

za artificiale. I volti delle vittime e dei sospetti vengono identificati e poi incrociati con i database nazionali dei passaporti e delle carceri. Questo approccio AI a più livelli consente un confronto approfondito con i registri ufficiali, portando all'identificazione precisa dei sospetti e al potenziale salvataggio delle vittime.

L'impatto di questa tecnologia è profondo. Solo l'anno scorso sono stati identificati oltre 200 sospetti grazie a questa tecnica combinata di intelligenza artificiale e riconoscimento vocale. Per mettere questo dato in prospettiva, le forze dell'ordine stimano che, senza questi strumenti avanzati, solo circa sei sospetti sarebbero stati identificati con i metodi tradizionali. Questo esempio sottolinea la potenza dell'integrazione dell'IA nel kit di strumenti delle forze dell'ordine. Evidenzia l'urgente necessità di cooperazione internazionale, di progressi tecnologici e di quadri giuridici solidi per sostenere questi approcci innovativi nella lotta al panorama in continua evoluzione della criminalità informatica.

L'ascesa dei siti web falsi: Un nuovo aspetto della criminalità informatica

Negli ultimi anni abbiamo assistito a un forte aumento dell'uso di siti web falsi come strumenti per la criminalità informatica. Questi siti web, che spesso imitano aziende, istituzioni finanziarie o agenzie governative legittime, sono progettati per ingannare gli utenti e indurli a fornire informazioni personali, scaricare malware o effettuare pagamenti fraudolenti. La sofisticazione di questi siti web falsi è allarmante: spesso presentano design realistici, URL dall'aspetto sicuro e persino interazioni finte con il servizio clienti per aumentare la loro credibilità.

La proliferazione di siti web falsi rappresenta una sfida significativa sia per le forze dell'ordine che per la magistratura. L'anonimato di Internet rende facile per i criminali informatici creare e gestire questi siti da qualsiasi parte del mondo, spesso utilizzando servizi di hosting in giurisdizioni con meccanismi di applicazione deboli. Una volta che questi siti vengono identificati e abbattuti, possono riapparire rapidamente con un altro nome o URL, rendendo il gioco del gatto e del topo per le autorità infinito.

Inoltre, l'impatto dei siti web falsi va oltre le perdite finanziarie per le vittime. Questi siti erodono la fiducia nei servizi digitali, rendendo le persone diffidenti nei confronti delle operazioni online legittime.

Il ruolo della giurisdizione penale nello spazio virtuale

Nell'affrontare queste sfide, una delle questioni centrali che dobbiamo affrontare è il ruolo della giurisdizione penale nello spazio virtuale. La crimi-

nalità informatica è intrinsecamente transnazionale e spesso coinvolge autori, vittime e prove distribuiti in più giurisdizioni. Le nozioni tradizionali di giurisdizione, basate sulla territorialità, sono sempre più inadeguate in questo contesto.

L'*InterPlanetary File System* (IPFS), ad esempio, è un protocollo e una rete *peer-to-peer* per l'archiviazione e la condivisione di dati in un *file system* distribuito. Rappresenta una svolta significativa rispetto alla tradizionale architettura web centralizzata, offrendo vantaggi unici in termini di distribuzione dei dati, resilienza e resistenza alla censura. Tuttavia, l'IPFS presenta anche sfide significative per le forze dell'ordine, in particolare nelle indagini sulla criminalità informatica.

A differenza del protocollo HTTP tradizionale, che si basa su server centralizzati, IPFS opera su una rete decentralizzata di nodi. Ogni nodo memorizza una parte dei dati complessivi e il contenuto viene recuperato utilizzando un sistema di indirizzamento basato sul contenuto piuttosto che sulla posizione. Ciò significa che si accede ai file in base al loro hash crittografico come identificatore univoco, e non alla loro posizione su un server specifico.

IPFS è un protocollo P2P, ovvero collega direttamente gli utenti per condividere i file. Quando un utente richiede un file, la rete lo recupera dal nodo più vicino o più veloce che ospita il file o parti di esso, piuttosto che da un singolo server centralizzato. Ciò consente di recuperare i file più velocemente e di ridurre i costi della larghezza di banda.

Per sua natura, IPFS è altamente resistente alla censura e alla perdita di dati. Poiché i dati sono distribuiti su numerosi nodi a livello globale, è quasi impossibile eliminare un contenuto specifico senza spegnere l'intera rete. Questo rende IPFS interessante per gli utenti che cercano di resistere alla censura dei dati, come gli attivisti o gli sviluppatori in regioni con politiche internet restrittive.

A causa della natura globale dell'IPFS, i contenuti illegali possono essere ospitati in più giurisdizioni, rendendo difficile l'applicazione efficace delle leggi nazionali. Anche se alcuni nodi sono situati in un Paese in cui determinati contenuti sono illegali, altri nodi possono esistere in Paesi in cui gli stessi contenuti non sono regolamentati, creando un'area grigia giurisdizionale.

L'efficacia della giurisdizione penale nello spazio virtuale dipende da diversi fattori, tra cui la capacità di attribuire i crimini informatici ad attori specifici, la volontà degli Stati di cooperare e la disponibilità di strumenti giuridici che possano essere efficacemente applicati in un ambiente digitale. Le discussioni in corso alle Nazioni Unite, in particolare il lavoro del Gruppo di lavoro aperto sulla criminalità informatica e i lavori preparatori per la Con-

venzione UNODC sulla criminalità informatica, sono fondamentali a questo proposito.

Queste discussioni non sono solo esercizi accademici, ma hanno implicazioni reali per il modo in cui rispondiamo alla criminalità informatica. La Convenzione UNODC sulla criminalità informatica mira a contribuire a definizioni più adeguate dei crimini informatici e a universalizzare i principi della cooperazione giudiziaria in materia penale, come stabilito nella Convenzione di Budapest e nel suo secondo Protocollo aggiuntivo. Tuttavia, affinché questi sforzi abbiano successo, devono essere informati dalla realtà della criminalità informatica e dalle sfide uniche poste dallo spazio virtuale.

Sicurezza informatica e sovranità nazionale

La criminalità informatica non è solo una questione penale, ma anche una questione di sicurezza e sovranità nazionale. Un attacco informatico alle infrastrutture critiche, ad esempio, può avere conseguenze devastanti per la sicurezza, l'economia e la sicurezza pubblica di una nazione. Tali attacchi richiedono una risposta coordinata che coinvolga non solo le forze dell'ordine, ma anche le agenzie di intelligence, gli esperti di sicurezza informatica e, in alcuni casi, le forze armate.

Il concetto di sovranità nel cyberspazio è ancora in evoluzione e c'è bisogno di regole e norme più chiare per governare il comportamento degli Stati in questo dominio. I Manuali di Tallinn, ad esempio, forniscono indicazioni preziose su come il diritto internazionale si applica alle operazioni informatiche, ma è necessario lavorare ancora per sviluppare un quadro giuridico completo che possa essere applicato universalmente.

L'importanza di un approccio globale

Le sfide che dobbiamo affrontare nella lotta alla criminalità informatica sono complesse e sfaccettate e richiedono un approccio globale che vada oltre i tradizionali metodi di applicazione della legge. Dobbiamo sfruttare le competenze di studiosi di diritto, tecnologi e politici per sviluppare soluzioni innovative in grado di tenere il passo con un panorama di minacce in rapida evoluzione.

Uno dei principali risultati della mia esperienza di procuratore che ha lavorato in casi di criminalità informatica per oltre dieci anni e che ora lavora presso Eurojust è la necessità di una maggiore integrazione delle attività di contrasto e giudiziarie a livello transfrontaliero.

Questa integrazione deve essere sostenuta da un solido quadro giuridico che faciliti la cooperazione, consenta la condivisione di informazioni e

prove in tempo reale e garantisca che i criminali informatici non possano sfruttare le lacune giurisdizionali per sottrarsi alla giustizia.

Allo stesso tempo, dobbiamo anche guardare al futuro e anticipare le sfide che si presenteranno con la diffusione di nuove tecnologie, come l'informatica quantistica. L'informatica quantistica ha il potenziale per rivoluzionare molte aree della scienza e della tecnologia, ma pone anche rischi significativi per la sicurezza informatica. La capacità dei computer quantistici di violare gli attuali metodi di crittografia potrebbe rendere obsolete molte delle nostre attuali misure di sicurezza, creando nuove opportunità per i criminali informatici.

Conclusioni

In conclusione, la lotta alla criminalità informatica non è solo una sfida legale o tecnica; è una sfida globale che richiede uno sforzo coordinato e sostenuto da parte di tutti noi. Dobbiamo continuare a basarci sui progressi compiuti, affrontare le lacune e i punti deboli dei nostri sistemi attuali e lavorare insieme per creare un mondo digitale più sicuro e protetto.

La cooperazione fluida ed efficiente tra le forze dell'ordine e la magistratura è essenziale per questo sforzo. Armonizzando i nostri quadri giuridici, rafforzando la cooperazione internazionale e regolamentando le tecnologie emergenti come l'IA, possiamo proteggere meglio le nostre società dalla minaccia sempre presente della criminalità informatica.

Cogliamo l'occasione per riaffermare il nostro impegno in questa causa e per lavorare insieme per costruire un futuro in cui lo Stato di diritto prevalga nel cyberspazio, proprio come nel mondo fisico.

Edvardas Sileris
Capo del Centro Europeo per i Crimini Cibernetici, Europol

È un piacere rivolgermi a voi illustri ospiti, colleghi e partner, oggi sul tema critico e attuale del cyberspazio, della criminalità informatica e dell'importanza di un'efficace cooperazione internazionale. Il panorama informatico continua a evolversi rapidamente, presentando sfide che richiedono risposte innovative e agili. Le minacce che affrontiamo sono più sofisticate che mai e la portata di queste sfide ci impone di lavorare insieme, al di là dei confini, dei settori e delle discipline.

Nel mondo interconnesso di oggi, i criminali informatici sfruttano le stesse tecnologie che consentono alle nostre società di prosperare. Dagli attacchi ransomware agli schemi di phishing e alle frodi nel commercio elettronico, queste attività sono spesso transnazionali e richiedono una risposta globale. È qui che la cooperazione multilaterale di polizia e giudiziaria, come quella coordinata da Europol e da altre istituzioni chiave, diventa indispensabile.

Adattamento alle minacce in evoluzione

Uno dei temi centrali della nostra lotta alla criminalità informatica è l'adattabilità. L'ecosistema criminale si è evoluto in modo significativo, influenzato dai progressi tecnologici e dai cambiamenti geopolitici. In questo ambiente dinamico, la nostra capacità di coordinarci rapidamente con un'ampia gamma di attori è fondamentale.

Per questo motivo la cooperazione di polizia è fondamentale. Con i partner europei e anche con altri attori internazionali, il Centro per la criminalità informatica di Europol (EC3) ha sviluppato un'ampia rete di supporto alle operazioni. Tali reti non solo facilitano la condivisione delle informazioni, ma contribuiscono anche allo sviluppo di valutazioni complete delle minacce, che guidano le nostre strategie nell'affrontare la criminalità informatica.

La Convenzione delle Nazioni Unite sulla criminalità informatica offre un importante quadro di partenza per la cooperazione giudiziaria, ma affronta anche aspetti chiave della collaborazione di polizia. In particolare, la Convenzione rafforza la cooperazione internazionale stabilendo principi condivisi per la criminalizzazione e la giurisdizione; introduce misure specifiche per le forze dell'ordine (così quelle relative ai principi generali della cooperazione, ai punti di contatto 24/7, alla cooperazione tra forze dell'ordine e alle indagini congiunte).

Questi punti di contatto, attivi 24 ore su 24 e 7 giorni su 7, sono attori essenziali nella lotta globale contro la criminalità informatica. Il loro ruolo

nell'elaborazione delle richieste e nello scambio di informazioni tra le diverse reti - che si tratti del G7, della Convenzione di Budapest, di INTERPOL o del sistema SIENA di Europol - non può essere sopravvalutato. Promuovendo questo scambio di informazioni in tempo reale, miglioriamo la nostra capacità di rispondere alle minacce informatiche in modo rapido ed efficace.

Sfruttare la Convenzione ONU per affrontare nuove sfide

La Convenzione delle Nazioni Unite ci fornisce un quadro di riferimento per rafforzare le capacità di applicazione della legge, in particolare nei Paesi che raggiungono il mondo. Questo è fondamentale nella nostra lotta contro le forme emergenti di criminalità informatica, come il ransomware, dove la cooperazione transfrontaliera è essenziale.

Una delle sfide continue nelle indagini sui crimini informatici, come quelli che coinvolgono il ransomware, è la necessità per le forze dell'ordine di accedere ai server dei criminali in giurisdizioni straniere. Come abbiamo visto in casi recenti, questi server sono spesso situati al di fuori di giurisdizioni affidabili, creando notevoli difficoltà alle agenzie che cercano di intervenire. La Convenzione delle Nazioni Unite può contribuire a mitigare queste sfide promuovendo una maggiore cooperazione e facilitando la condivisione delle prove a livello transfrontaliero.

Inoltre, la Convenzione offre nuove opportunità per impegnarsi con i Paesi in cui le attività di criminalità informatica, come la *sextortion* e le frodi nel commercio elettronico, sono prevalenti. In regioni come l'Africa occidentale e alcune parti dell'Asia, la cooperazione è fondamentale per identificare i colpevoli e mitigare le attività criminali come le truffe amorose e lo sfruttamento dei minori.

Anche la crescente minaccia della criminalità guidata dall'intelligenza artificiale richiede la nostra attenzione. Man mano che l'intelligenza artificiale diventa più accessibile ai criminali, il suo potenziale di aumentare la sofisticazione e la portata della criminalità informatica è allarmante. Dai deepfake utilizzati per le frodi e i furti d'identità agli strumenti di intelligenza artificiale impiegati negli attacchi di ingegneria sociale, dobbiamo prepararci a questa nuova frontiera. La Convenzione delle Nazioni Unite offre un punto di partenza per sviluppare tutele contro queste minacce guidate dall'IA, in particolare nei casi di impersonificazione di deepfake o di produzione di materiale pedopornografico.

Basarsi sulle migliori pratiche

Europol è da tempo un laboratorio di buone pratiche nella cooperazione di polizia, che si adatta continuamente alle nuove minacce. Il Centro europeo

per la criminalità informatica (EC3), ad esempio, ha introdotto approcci innovativi al coordinamento operativo, come testimoniato dalla Task Force congiunta per la criminalità informatica (JCAT) e da iniziative come l'Unità di riferimento per Internet (IRU). Questi sforzi hanno portato a successi significativi nel mitigare l'impatto delle minacce informatiche su larga scala, tra cui il ransomware e le piattaforme Darknet come Raidforum.

I partenariati pubblico-privato sono un'altra pietra miliare del nostro successo. Collaborando con gli operatori del settore e altre parti interessate, Europol è stato in grado di fornire soluzioni globali sia alle vittime che agli attori operativi. Operazioni come la bonifica di EMOTET e azioni di takedown come PowerOff dimostrano l'efficacia di queste partnership nel neutralizzare le infrastrutture criminali.

Tuttavia, al di là della Convenzione delle Nazioni Unite, dovranno ancora essere risolte sfide importanti. I quadri giuridici sono solo una parte della soluzione. L'accesso ai dati, in particolare l'accesso transfrontaliero, rimane un ostacolo significativo per le forze dell'ordine. La possibilità di recuperare prove da fornitori di cloud o da server situati in giurisdizioni straniere dipende spesso da un mosaico di accordi legali, standard e di cooperazione.

Per superare questi ostacoli, dobbiamo garantire che la cooperazione si estenda oltre le forze dell'ordine, includendo il settore privato e altre comunità. I futuri successi nella lotta alla criminalità informatica dipenderanno dalla nostra capacità di creare una sinergia tra queste diverse parti interessate, di stabilire standard tecnologici amichevoli e di promuovere pratiche proattive di condivisione delle informazioni.

Guardare avanti: Risultati promettenti e strada da percorrere

Stiamo già vedendo i risultati della cooperazione rafforzata tra le forze di polizia nella lotta contro la criminalità informatica. Le recenti operazioni sostenute da Europol a livello internazionale ed europeo sono state emblematiche di ciò che si può ottenere quando si lavora insieme. Ad esempio, gli sforzi coordinati hanno portato allo smantellamento di gruppi organizzati di criminalità informatica, all'interruzione di infrastrutture criminali chiave e persino all'abbattimento di importanti piattaforme Darknet.

Tuttavia, si può fare di più. Guardando al futuro, dobbiamo continuare a costruire su questi successi. La Convenzione delle Nazioni Unite sulla criminalità informatica è uno strumento promettente, ma il suo vero potenziale potrà essere realizzato solo se riusciremo ad affrontare le sfide rimanenti, ovvero facilitare l'accesso ai dati da parte delle forze dell'ordine e promuove-

re una maggiore cooperazione internazionale in tutti i settori.

In conclusione, la criminalità informatica è una minaccia globale che richiede una risposta globale. Con i giusti quadri giuridici, il coordinamento operativo e la cooperazione transfrontaliera, possiamo ridurre significativamente l'impatto della criminalità informatica e proteggere le nostre società da queste minacce in continua evoluzione. Continuiamo a innovare, a collaborare e a costruire le capacità necessarie per garantire un mondo digitale più sicuro per tutti.

DIBATTITO

Eugenio Albamonte:

Mi preme valorizzare alcuni degli stimoli emersi dagli interventi appena ascoltati, quali le prospettive di implementazione, la maggiore operatività congiunta degli attori investigativi sul campo, la condivisione delle nuove tecnologie applicate alle investigazioni, e ciò per fare in modo che tutte le istituzioni – forze di polizia e autorità giudiziarie – abbiano una capacità di azione omogenea nell'ambiente informatico; ed ancora, la omogeneizzazione di approccio, la quale non deve riguardare solo il regime di conservazione e accesso ai dati informatici, ma anche gli standard utilizzati dalle diverse forze di polizia per la raccolta e l'analisi dei dati. È altresì importante assicurare l'efficacia dello scambio di informazioni e l'azione attiva della polizia nel cyberspazio, non solo in modo reattivo, ma anche preventivo. Entrano qui in gioco, in altri termini, non solo le investigazioni finalizzate all'individuazione e alla repressione degli autori dei reati, ma altresì la funzione preventiva delle forze dell'ordine. In tal senso, una volta individuate infrastrutture inevitabilmente malevoli, sarebbe necessario poter intervenire su di esse prima che vengano utilizzate per commettere reati.

Vorrei offrire un ulteriore spunto alla vostra riflessione.

Esso riguarda l'importante slancio dato dall'articolo 32 della Convenzione di Budapest sulla Criminalità informatica, che ha consentito la cooperazione diretta, informale e destrutturata tra pubblico e privato, cioè tra lo Stato, le forze di polizia, i pubblici ministeri e gli Internet Service Provider, nell'acquisizione e raccolta di dati fondamentali per l'individuazione dei soggetti in tempi rapidi.

L'articolo 32 ha anche un'altra portata, permettendo l'uso della rete per svolgere indagini attraverso il cyberspazio, anche in luoghi che potrebbero essere sottratti alla giurisdizione statale. È grazie a questo strumento che, diversi anni fa, quale Pubblico Ministero nell'ambito di un'indagine su reati informatici ho potuto svolgere un'ispezione informatica su server esteri, operata dall'Italia, per verificare se determinati server di Google ospitassero contenuti criminali. Si tratta di forme di cooperazione spontanea, molto informali, che però ampliano notevolmente la dimensione, l'operatività e la tempestività delle nostre azioni.

Se questa positiva esperienza nel rapporto tra soggetti pubblici e privati potesse essere estesa anche ai rapporti tra soggetti pubblici, tra Stati, tra

autorità giudiziarie e forze di polizia giudiziaria, sarebbe un passo avanti importante.

Ivano Gabrielli:

Nel cogliere quest'ultimo spunto, mi preme segnalare che quali autorità di contrasto nel tempo abbiamo tratto sempre maggiore vantaggio da una cooperazione volontaria, che ha visto operare plurimi soggetti al di fuori dei confini geografici e politici, erogando servizi e gestendo clientele che esulano dai confini nazionali. Tali attori hanno aderito a modelli di cooperazione pubblico-privato rivelatisi molto produttivi e proficui. Purtroppo, a fianco a questi modelli positivi, abbiamo altresì sperimentato situazioni in cui è stato sistematicamente negato l'accesso a operazioni legittime, con conseguente spazio libero ad ambiti di illegalità evidenti e riconoscibili.

Oggi è necessario fare un salto di qualità. L'universalità di uno strumento come una Convenzione ONU sul cybercrime ci permette di guardare a modalità di cooperazione che non si basano più solo su adesioni volontaristiche, ma legittimano forme di cooperazione tra Stati. In breve, dobbiamo trovare forme di cooperazione che superino il modello fondato su "congelamento" e successiva acquisizione dei dati, passando a una cooperazione attiva e dinamica, cooperazione questa che richiede necessariamente anche il mutuo riconoscimento degli strumenti investigativi.

La velocità con cui si muovono gli assetti del cybercrime oltre i confini pone la necessità di essere rapidi nel ricercare prove, anche attraverso strumenti investigativi efficaci quali quelli già in uso nel contrasto alla pedopornografia e alle forme più aggressive di criminalità informatica. Ci si riferisce alle attività undercover (sotto copertura), che spesso si spostano in spazi virtuali non definiti, non allocabili dal punto di vista geografico e quindi non facilmente riconducibili alla giurisdizione di un singolo Stato.

Lo spazio cibernetico è uno spazio condiviso, dove si muovono, con estrema rapidità, sia economie legittime sia criminali. Le organizzazioni criminali hanno risorse significative, conoscono le legislazioni e riescono a adattare le loro attività ai cambiamenti normativi internazionali e alle capacità di reazione di alcuni paesi.

È fondamentale, dunque, avere una cooperazione veloce, che passi attraverso un riconoscimento preliminare delle capacità di acquisizione delle prove, prove che poi possano essere validate dalle Autorità giudiziarie. Occorre, in altri termini, tendere verso un approccio rivolto a sfruttare meglio la capacità operativa dei vari paesi, consentendo in primo luogo alle rispettive forze di polizia di partecipare ad attività investigative comuni, agendo velocemente quando la gravità di un crimine lo giustifica, per poi far validare

l'acquisizione probatoria compiuta attraverso un controllo da parte della Autorità giudiziaria.

Tutto ciò diventa essenziale, per esempio, per contrastare fenomeni come la produzione, la vendita e la diffusione di materiale pedopornografico. A mio avviso, dobbiamo essere in grado di agire anche a distanza, portando avanti attività investigative con rapidità, mettendo in atto sforzi proattivi per contrastare forme di criminalità così multiformi, veloci e adattabili rispetto al panorama e al framework legale internazionale.

Hannes Glantschnig:

Anch'io vorrei sottolineare che la velocità nelle indagini è un valore fondamentale, come indicato in un articolo della Convenzione di Budapest sulla criminalità informatica.

A monte, però, molte delle informazioni che condividiamo a livello di polizia con Europol e Interpol creano un problema di utilizzabilità al pubblico ministero, poiché tali informazioni hanno spesso natura di *intelligence* e non possono essere dunque utilizzate nel processo. Di conseguenza, sovente non si riescono ad ottenere mandati di arresto proprio perché la fonte sarebbe costituita da dati di *intelligence*. È necessario, pertanto, creare le premesse per la emissione di ordini o mandati a livello europeo affinché queste informazioni possano essere utilizzate come prova in giudizio.

Tornando al fattore "rapidità", si è certamente cercato di velocizzare i processi, ma siamo ancora nella fase in cui dobbiamo stampare, firmare e spedire documenti con modalità tradizionali. A volte si inviano perfino i fax, modalità non più comune in molti Paesi, ma si sta lavorando su un nuovo sistema per inviare informazioni con modalità elettronica per garantirne celeri invio e ricezione. Tuttavia, resta il problema del tempo per le traduzioni linguistiche. In futuro, potremmo avere la traduzione automatica, ma se oggi un criminale apre un conto in ogni paese europeo e trasferisce fondi da un conto all'altro, seguirli con un metodo tradizionale potrebbe richiedere troppo tempo per dare risultati proficui.

Esiste, tuttavia, la possibilità di aggirare la lentezza di una simile procedura attraverso lo *scambio spontaneo di informazioni*: attraverso Eurojust si possono scambiare informazioni senza che sia necessaria la traduzione nell'altrui lingue nazionale, e queste informazioni possono essere condivise con qualsiasi Paese[51]; si tratta di un meccanismo assai comodo e utile, che

51 Ci si riferisce all'art. 21 del Regolamento UE 2018/1727 istitutivo e regolare dell'agenzia EUROJUST, intitolato "Scambio di informazioni con gli Stati membri e tra membri nazionali", il quale prevede, tra l'altro, che le autorità competenti degli Stati membri scambiano con Eurojust tutte le informazioni necessarie allo svolgimento dei suoi compiti, …tra le quali le informazioni

andrebbe meglio conosciuto e valorizzato.

Ed ancora, la velocità è essenziale, ma anche la *gestione delle informazioni sui provider* è fondamentale.

Spesso nelle indagini ci si trova di fronte a provider di servizi mai incontrati prima, che non sono nemmeno nominati; non si sa che tipo di dati esso conserva, dove si possono ottenere e per quanto tempo verranno conservati. Inoltre, non è chiaro che tipo di informazioni vengano richieste per poter accedere a questi dati. Per la maggior parte dei provider, abbiamo informazioni su cosa e a quale indirizzo inviare, e per quanto tempo le informazioni richieste saranno disponibili. Se si vogliono informazioni da un provider, c'è una procedura strutturata da seguire e non è necessario cercare le informazioni sulle loro homepage. Si tratta di un profilo molto importante, che va conosciuto.

Come agenzia Eurojust svolgiamo anche attività formativa e sviluppiamo schede informative. Se si necessita, per esempio, di inviare una richiesta di assistenza giudiziaria al Giappone, è possibile trovare un format di richiesta già predisposta

Edvardas Sileris:

Parlando di criticità, è doveroso sottolineare che talvolta, per esempio, le forze di polizia non possono agire efficacemente perché i dati sono di proprietà di privati. Per affrontare e superare tale impasse, nel Centro di Cybercrime di Europol abbiamo creato dei gruppi di consulenza per acquisire anche il know-how degli enti privati. Fino ad ora, abbiamo avuto successo e siamo efficienti, includendo sempre di più i privati nelle nostre attività. Ma talvolta le difficoltà restano.

Vi vorrei fare l'esempio degli attacchi ransomware, ove tale criticità si sperimenta con frequenza: solitamente, quando c'è una vittima di un attacco ransomware, chi reagisce è il settore privato, non le forze di polizia, perché queste ultime non sanno come aiutare la vittima. In altri termini, noi autorità di contrasto sappiamo che c'è un attacco in corso, ma non conosciamo l'infrastruttura né il software che stanno attuando l'attacco. Questo significa che sono le aziende di cybersecurity a intervenire per risolvere il problema all'impresa aggredita. Non disponiamo poi di protocolli unificati su come racco-

sulla istituzione di squadre investigative comuni, i casi in cui sono state attivare forme di assistenza giudiziaria verso almeno due Stati membri; e ancora che gli stessi membri nazionali scambiano tra loro o con le autorità nazionali competenti, senza autorizzazione preliminare, tutte le informazioni necessarie allo svolgimento dei compiti di Eurojust. In particolare, le autorità nazionali competenti informano senza ritardo i rispettivi membri nazionali dei casi che li riguardano [N.D.R.]

gliere dati d'interesse dal settore privato, per potere arrivare al centro di controllo dell'attacco. Perciò, come detto, sono i privati a reagire per primi e poi, solo eventualmente, intervengono le forze di polizia.

Occorre capire come affrontare il problema e cosa può essere utile per l'indagine penale, perché in molti casi non ci vuole molto tempo. I privati dovrebbero raccogliere dati con nuovi indirizzi IP, dati che a loro volta potrebbero contenere informazioni di grande valore per gli inquirenti. Si potrebbero da ciò individuare i legami con un gruppo criminale, responsabile dell'attacco, e di lì approdare a degli arresti in futuro.

Il mio messaggio è pertanto che i partner privati sono cruciali e dobbiamo trovare i modi migliori per ottenere informazioni in modo efficiente da loro e ridurre il più possibile gli appesantimenti burocratici del nostro modo di agire

TERZA SESSIONE

UNA GIURISDIZIONE EFFICACE NEI CRIMINI INFORMATICI TRANSNAZIONALI

UNA GIURISDIZIONE EFFICACE NEI CRIMINI INFORMATICI TRANSNAZIONALI

PRESIEDE

Luigi Salvato
Procuratore Generale della Corte di Cassazione

Nell'aprire quest'ultima sessione, per il tempo ed il compito affidatomi mi limito ad osservare che la rivoluzione tecnologica va governata con norme efficaci ed effettive, caratteri garantiti anche dalla giurisdizione, messa in crisi dal cyberspazio.

La giurisdizione è infatti una competenza espressione della sovranità, principale attributo degli Stati. Costituisce un caposaldo del diritto internazionale la norma consuetudinaria sulla sovranità territoriale: lo Stato gode di una giurisdizione esclusiva nell'ambito del suo territorio ed è illecito per il diritto internazionale qualsiasi esercizio non autorizzato del potere nel territorio altrui.

I confini spazio-temporali sono stati però sbriciolati dal cyberspazio. Sua caratteristica è la a-territorialità, esaltata dalla condizione di anonimato, garantita dal ricorso a soluzioni crittografiche, causa della cd. *loss of location*, che rende complicato stabilire "chi", "come" e "dove" di un'azione cyber-criminale. Nel cyberspazio gli Stati nazionali sembrano, inoltre, perdere forza rispetto alle grandi imprese che gestiscono infrastrutture transnazionali, costituite da vari segmenti, i quali sfuggono alla territorializzazione, elemento costitutivo della sovranità ed aspetto primario dell'esercizio della giurisdizione e del diritto che regola i rapporti fra Stati.

Eppure, lo spazio virtuale resta comunque uno spazio materiale agganciato al territorio. Qualsiasi dato informatico, in ultima istanza, deve necessariamente essere memorizzato su un supporto fisico. Ritenendo commesso nello Stato un reato, quando nel territorio nazionale si è realizzata l'azione o l'omissione, o almeno una parte della condotta o dell'evento – secondo una regola stabilita nell'ordinamento italiano dall'art. 6 cod. pen. – la questione è quella delle azioni che la rendono effettiva. Sono queste che vengono in urto con la sovranità di altri Stati, con altre giurisdizioni e rendono complicata una difesa mediante strutture di cibersicurezza costituite all'interno dei singoli Stati.

Il carattere transnazionale del cybercrime ha dimostrato l'insufficienza dello strumento della rogatoria, tradizionale strumento di dialogo del diritto

internazionale, ma fra Stati, non fra autorità giudiziarie, che assicura un controllo nel proprio ambito sovrano, ma non dà certezza nella risposta, non garantisce agilità e rapidità nell'esecuzione.

Il cyberspazio esige il ripensamento di tradizionali istituti giuridici, finalità che conforta l'attualità del pensiero e dell'attività di Vittorio Occorsio, nel cui nome opera la Fondazione organizzatrice dell'evento che ci vede riuniti. Come ha scritto Giovanni Salvi, Vittorio Occorsio era giunto ad importanti risultati, «perché non si era acquietato nell'utilizzo delle categorie interpretative correnti» ed «aveva operato, insieme ad altri colleghi, in maniera innovativa».

Nella capacità di adeguamento e di innovazione degli istituti giuridici devono trovare risposta le sfide poste dalla rivoluzione scientifica.

L'obiettivo è dare effettività alla norma, di cui è insostituibile presidio la giurisdizione e che, assicurandola attraverso il processo, garantisce i diritti fondamentali, senza discriminazione, ed il ragionevole bilanciamento degli stessi con i doveri fissati dalle norme penali.

La comunità internazionale, pur con note difficoltà, sta elaborando risposte ispirate a tale convincimento, mediante l'evoluzione degli strumenti di cooperazione giudiziaria, che ha trovato svolgimento all'interno del Consiglio d'Europa, dell'Unione europea e dell'ONU.

Gli interventi di oggi faranno il punto su tale evoluzione, sulle strategie in grado di garantire l'efficacia della giurisdizione, ma anche sulle strategie di indagine che hanno un compito autonomo, di presidio preventivo della sicurezza, e concorrente, in quanto si inseriscono all'interno del processo.

DIRITTO INTERNAZIONALE E CONTROMISURE IN RISPOSTA A OPERAZIONI CYBER PROVENIENTI DA ALTRI STATI

Marco Roscini

Professore di Diritto Internazionale presso l'Università di Westminster - Londra e Professore di Diritto internazionale umanitario presso la Geneva Academy of International Humanitarian Law and Human Rights

Immaginiamo il seguente scenario, peraltro molto frequente: da uno Stato straniero vengono condotte operazioni informatiche malevole contro l'Italia o le aziende italiane, ad esempio per interrompere il funzionamento di infrastrutture cablate o per acquisire segreti industriali. Non vi è certezza chi ne sia il responsabile. La sola circostanza nota è che provengono da infrastrutture informatiche situate in un determinato Stato estero. Quello di cui vorrei parlare è se il diritto internazionale consenta allo Stato vittima di affrontare il problema alla radice, cioè intervenendo direttamente sul territorio dello Stato da cui proviene la minaccia informatica.

Questa azione costituirebbe un esercizio di giurisdizione extraterritoriale. La giurisdizione esecutiva extraterritoriale nel cyberspazio può essere esercitata per accedere ed estrarre dati memorizzati su *server* o computer stranieri, al fine di raccogliere le prove necessarie per stabilire la responsabilità di uno Stato o per utilizzarle in procedimenti penali. La giurisdizione esecutiva extraterritoriale può anche assumere la forma di *hacking back* per chiudere i *server* stranieri utilizzati per condurre le operazioni o per disinfettare i *bot*.

Il diritto internazionale consente l'esercizio della giurisdizione extraterritoriale? In questo contesto entrano in gioco diverse norme di diritto internazionale, le principali delle quali sono la norma che tutela la sovranità territoriale e il principio di non intervento negli affari interni di altri Stati. Non sorprende che l'articolo 5 della bozza di Convenzione ONU sulla criminalità informatica richiami entrambe e avverta che, di norma, nessuna disposizione della Convenzione autorizza gli Stati a esercitare la giurisdizione e a svolgere funzioni sovrane sul territorio di altri Stati.

Partendo dalla norma che tutela la sovranità territoriale, la sovranità è un principio fondamentale del diritto internazionale, che - almeno a partire dalla Pace di Westfalia del 1648 - ha una connotazione strettamente territoriale: l'ordine internazionale è organizzato attorno a una moltitudine di Stati, che possono esercitare un'autorità sovrana su una porzione della superficie terre-

stre escludendo gli altri Stati. Questa autorità è esattamente ciò che chiamiamo "giurisdizione" ed è normalmente esercitata da uno Stato sugli individui, sulle loro condotte, e sulle infrastrutture all'interno del territorio nazionale. La giurisdizione può consistere nell'emanazione, modifica e revoca di norme vincolanti (giurisdizione prescrittiva), nell'attuazione di tali norme vincolanti (giurisdizione esecutiva) e nella risoluzione delle controversie che ne derivano (giurisdizione giudiziaria). Come già detto, le ricerche investigative e l'attività di *hacking back* sono un esempio di giurisdizione esecutiva.

Ciò che il diritto internazionale dice in merito all'esercizio extraterritoriale della giurisdizione è ancora contenuto nella classica sentenza Lotus del 1927 della Corte permanente di giustizia internazionale, dove la Corte distingue l'esercizio della giurisdizione esecutiva da altre forme di giurisdizione (Caso Lotus, Francia contro Turchia, Corte Permanente Internazionale di Giustizia, 1927). Mentre uno Stato non può esercitare "il suo potere in qualsiasi forma" (cioè la giurisdizione esecutiva) nel territorio di un altro Stato senza il suo consenso o senza una norma permissiva di diritto internazionale, può "estendere l'applicazione delle [sue] leggi e la giurisdizione dei [suoi] tribunali a persone, beni e atti al di fuori del [suo] territorio" a meno che non vi sia una norma proibitiva di diritto internazionale. Quindi l'esercizio della giurisdizione esecutiva extraterritoriale è vietato a meno che non sia consentito, mentre l'esercizio della giurisdizione prescrittiva/giudiziaria extraterritoriale è consentito a meno che non sia vietato. La ragione di questo diverso trattamento è che l'esercizio extraterritoriale della giurisdizione esecutiva è un esercizio molto più invasivo dell'autorità sul territorio dello Stato destinatario rispetto all'adozione di leggi e atti giudiziari. L'eccesso di giurisdizione prescrittiva e il rigido approccio territoriale della giurisdizione esecutiva possono creare un vuoto di applicazione particolarmente evidente nello spazio virtuale.[52]

Al fine di scongiurare violazioni della sovranità territoriale dello Stato dal quale origina l'attività malevola, pertanto, lo Stato che intende rispondere a tale attività attraverso azioni di *hacking back* avrà bisogno di una base giuridica per condurre sia la risposta, che le eventuali attività di indagine transfrontaliere: infatti, anche se i dati risultano archiviati "nel cloud", essi esistono ancora in uno o più server fisici situati nel territorio di qualche Stato. La necessaria base giuridica potrebbe essere tanto il consenso concesso dall'au-

52 Kohl, 76. La legge sul cloud statunitense estende la giurisdizione degli Stati Uniti su tutti i dati controllati dalle piattaforme locali, indipendentemente dalla loro ubicazione. Ciò consente di colmare il divario di applicazione tra la portata eccessiva della giurisdizione prescrittiva e il rigido approccio territoriale della giurisdizione esecutiva.

torità competente dello Stato territoriale a seguito di una richiesta ad hoc; quanto un trattato in vigore tra gli Stati interessati, che consenta ad uno Stato parte di effettuare attività di *hacking back* ovvero attività di indagine sulle infrastrutture cyber di un altro Stato parte (in assenza di un ulteriore consenso *ad hoc)*. Una via di mezzo è l'articolo 32 della Convenzione di Budapest sulla criminalità informatica, che prevede che una parte possa accedere o ricevere dati informatici memorizzati situati in un'altra parte senza la sua autorizzazione, ma solo se ha il consenso legittimo e volontario della persona che ha la legittima autorità di divulgare i dati attraverso quel sistema informatico. In definitiva, tuttavia, gli Stati devono fare affidamento sul consenso degli Stati e, quindi, sui trattati di cooperazione internazionale e di mutua assistenza legale per applicare le loro leggi a livello extraterritoriale, e il cyberspazio non fa eccezione.

Interpretazioni meno restrittive al divieto generale all'esercizio extraterritoriale della giurisdizione prescrittiva, sono più frequenti nei Paesi occidentali, mentre osteggiate da parte di quei Paesi che esercitano uno stretto controllo statuale sullo spazio cyber. Da tale approccio deriva che le prove digitali sono considerate analoghe ad ogni altro genere di prova. Non si è quindi ancora formata un'eccezione consuetudinaria al principio di Lotus per le ricerche investigative extraterritoriali nel cyberspazio, e questo è ancora più vero per l'*hacking back* che mira a chiudere i *server* all'estero.[53]

Le azioni esecutive transfrontaliere nel cyberspazio senza una base giuridica o una norma permissiva di diritto internazionale non solo costituirebbero una violazione della sovranità territoriale dello Stato bersaglio, ma potrebbero anche integrare una violazione del principio di non intervento. Questo principio è una delle regole più antiche del diritto internazionale, in quanto è un corollario della sovranità statale. Protegge gli Stati da qualsiasi atto coercitivo nei loro affari interni (ed esterni), cioé vieta agli Stati di costringere altri Stati a fare qualcosa che hanno il diritto di non fare e a non fare qualcosa che hanno il diritto di fare. Le operazioni di hack *back* e le attività di indagine extraterritoriali effettuate senza il consenso dello Stato potrebbero essere qua-

53 Paesi Bassi 2019: "L'atto di esercitare poteri investigativi in un contesto transfrontaliero è tradizionalmente considerato una violazione della sovranità di un Paese, a meno che il Paese in questione non abbia esplicitamente concesso l'autorizzazione... Le opinioni sono discordanti su cosa si qualifichi come esercizio di poteri investigativi in un contesto transfrontaliero e su quando sia ammissibile senza una base giuridica fondata su un trattato. Anche nel cyberspazio, le prassi dei Paesi differiscono nei loro approcci pratici al principio di sovranità in relazione alle indagini penali". Posizione comune dell'UA: "autorità esecutiva sul territorio di uno Stato straniero ... anche se l'esercizio di tale autorità esecutiva da parte di uno Stato non ha effetti dannosi, virtuali o fisici, sul territorio di uno Stato straniero".

lificate come coercitive ove impongano una condizione (chiusura dei *server*, esfiltrazione di informazioni non pubbliche conservate sul territorio) allo Stato bersaglio.

Quindi, l'esercizio extraterritoriale della giurisdizione esecutiva attraverso l'*hacking back* è vietato da almeno due norme di diritto internazionale. Questo significa che non possiamo fare nulla per fermare le operazioni informatiche dannose provenienti dall'estero o per raccogliere prove su di esse quando queste prove sono conservate in computer e *server* all'estero e lo Stato territoriale si rifiuta di collaborare? In assenza di una base giuridica permissiva, la nostra risposta extraterritoriale sarà illegale ai sensi del diritto internazionale, ma questa illegalità potrebbe essere preclusa dal fatto che è stata adottata contro un precedente atto illecito commesso contro di noi da un altro Stato. Questa è la dottrina delle contromisure, che ha una solida base nel diritto internazionale consuetudinario, come confermato anche nel documento di posizione italiano sull'applicazione del diritto internazionale nel cyberspazio[54]. Le contromisure sono un meccanismo di applicazione del diritto: tu violi gli obblighi di diritto internazionale nei miei confronti, io violo gli obblighi di diritto internazionale nei tuoi confronti, al fine di attuare la tua responsabilità in quanto Stato che ha commesso l'illecito. Questo è di fatto il modo in cui viene applicata la maggior parte del diritto internazionale.

Il problema principale dell'utilizzo della dottrina delle contromisure per giustificare attività di *hackig back* o indagini extraterritoriali non autorizzate è che richiede un precedente atto illecito commesso da un altro Stato. Nella maggior parte dei casi, tuttavia, le operazioni dolose saranno condotte da gruppi criminali senza il coinvolgimento di uno Stato. Anche se uno Stato ne è responsabile, sarà probabilmente difficile dimostrare la sua responsabilità con "un sufficiente livello di affidamento" (per usare il linguaggio del documento di posizione italiano sull'applicazione del diritto internazionale nel cyberspazio).

Nei casi in cui lo Stato da cui provengono le operazioni informatiche non sia responsabile, o non possa essere provato, sostengo che si possa ancora giustificare l'esercizio extraterritoriale della giurisdizione esecutiva sul suo territorio sulla base della dottrina delle contromisure, se si tiene conto della regola della dovuta diligenza (*due diligence*). Questa regola di diritto internazionale impone agli Stati di evitare che il loro territorio venga utilizzato per la commissione di atti contrari ai diritti di altri Stati. Affinché uno Stato possa essere considerato responsabile della violazione di tale norma, è necessario che lo stesso: 1) sia a conoscenza della circostanza che le proprie infrastruttu-

54 Italian position paper on international law and cyberspace, 2021.

re cyber siano utilizzate per condurre operazioni cyber contro altri Stati dalle quali derivino gravi conseguenze per gli Stati stessi; e 2) non abbia adottato tutte le misure possibili, nelle circostanze del caso, per porvi fine. La due diligence ci permette di aggirare le difficoltà tecniche associate all'attribuzione nello spazio virtuale, in quanto non è necessaria l'attribuzione delle operazioni informatiche a uno Stato, ma è la responsabilità per l'omissione di un'azione, piuttosto che la responsabilità per l'azione stessa. Il nostro *hack back* per spegnere i server sarebbe quindi una risposta alla mancata adozione da parte dello Stato territoriale di tutte le misure possibili per porre fine alle operazioni informatiche contro di noi da quei server. Nel caso di una ricerca investigativa, le prove che intendiamo ottenere devono essere necessarie per fermare le operazioni dannose che lo Stato territoriale non è disposto a terminare e/o per impedirne la ripetizione.

Questo argomento, tuttavia, presenta due potenziali punti deboli. In primo luogo, non tutti gli Stati ritengono che la *due diligence* sia una vera e propria norma vincolante del diritto internazionale e preferiscono vederla come una semplice norma di comportamento responsabile - come qualcosa che gli Stati dovrebbero, non devono, fare: in quanto tale, gli Stati non violerebbero il diritto internazionale se non la rispettano e non ci sarebbe alcun atto illecito a cui rispondere con contromisure. Tuttavia, la maggioranza degli Stati, tra cui l'Italia, considera la dovuta diligenza una regola vincolante, anche se non è chiaro quanto danno debba essere causato perché questa regola venga violata. In secondo luogo, storicamente le contromisure sono state interpretate come misure da Stato a Stato, ovvero devono essere adottate dallo Stato leso e dirette contro lo Stato responsabile per indurlo a rispettare l'obbligo violato: quando le operazioni informatiche dolose sono condotte da gruppi criminali dall'estero senza il coinvolgimento dello Stato territoriale, si potrebbe dire che spegnere i *server* che utilizzano o accedere a dati non pubblici per perseguirli è una reazione contro il gruppo criminale stesso, e non contro lo Stato territoriale. Questo punto di vista, tuttavia, non è persuasivo. Anche se il gruppo criminale sarebbe il bersaglio finale della nostra risposta, è il diritto dello Stato da cui opera che viene violato dall'azione di contrasto transfrontaliera (vale a dire, la sua sovranità territoriale e il suo diritto a non essere costretto in base al principio di non intervento). Le misure sono quindi adottate "contro" lo Stato territoriale. Inoltre, la legge può cambiare, e forse sta cambiando, per affrontare le nuove realtà dello spazio virtuale. Se la concezione tradizionale delle contromisure è quella di indurre lo Stato inadempiente a conformarsi alla legge, un approccio più moderno prevede che esse possano anche sostituire o integrare ciò che lo Stato dovrebbe fare in base al diritto internazionale: le contromisure, in altre parole, servono ad attuare la

responsabilità dello Stato per le violazioni del diritto internazionale, compresa la dovuta diligenza, obbligando lo Stato responsabile a ripristinare lo *status quo* giuridico o consentendo allo Stato leso di farlo da solo. Si tratta di un ampliamento della concezione tradizionale della dottrina delle contromisure che potrebbe essere reso necessario dalle caratteristiche dello spazio virtuale, tra cui le difficoltà di attribuzione e il ruolo di primo piano svolto dagli attori non statali. A mio avviso, questo ampliamento è ancora in linea con la logica delle contromisure, ovvero l'attuazione della responsabilità dello Stato.

Va da sé che tutti i requisiti previsti dalla legge sulle contromisure devono essere rispettati, in particolare gli effetti della nostra risposta devono essere reversibili, ove possibile, e devono essere proporzionati al danno subito. In caso di contromisure in risposta a una violazione della dovuta diligenza, la proporzionalità dovrà essere valutata in relazione all'omissione dello Stato territoriale di adottare tutte le misure fattibili per porre fine alle operazioni informatiche dal suo territorio, e non alle conseguenze delle operazioni informatiche dei gruppi criminali cui lo Stato territoriale non ha posto fine.[55]

Per concludere, anche se l'esercizio extraterritoriale della giurisdizione esecutiva nello spazio virtuale è ancora illegale ai sensi del diritto internazionale consuetudinario, allo stesso modo in cui è illegale nel mondo analogico, in alcune circostanze questa illegalità può essere esclusa dal fatto che l'esecuzione transfrontaliera può essere interpretata come una contromisura contro un precedente atto illecito commesso dallo Stato da cui provengono le operazioni informatiche contro di noi, sia perché tale Stato ne è responsabile, sia perché ha violato l'obbligo di diligenza di porvi fine. Tuttavia, anche quando è lecito, dobbiamo sempre tenere presente i costi politici dell'esercizio di poteri esecutivi extraterritoriali sul territorio di un altro Stato senza il suo consenso. Detto altrimenti, qualsiasi "espansione dei poteri di hacking per l'applicazione della legge .... dovrebbe bilanciare gli interessi dell'applicazione della legge con le relazioni estere e gli interessi di sicurezza nazionale concorrenti"

55 Manuale di Tallinn, 130.

LA DISINFORMAZIONE. UNA REGOLAZIONE POSSIBILE DEGLI STRUMENTI DI TUTELA

Oreste Pollicino
Professore Ordinario di Diritto Costituzionale Università Bocconi

Non c'è dubbio che oggi più che mai i tribunali si trovino in una posizione privilegiata per individuare i rischi di potenziale collisione tra regimi giuridici interconnessi in termini di tutela dei diritti fondamentali. La cooperazione tra tribunali crea legami più stretti tra ordinamenti diversi ma interagenti, contribuendo al contempo ad adattare i sistemi giuridici alle nuove sfide globali. L'importanza di questa dinamica - e, più in generale, del ruolo e dell'impatto dell'attività giudiziaria - è ancora maggiore nel dominio digitale. Quali sono le ragioni di questa "amplificazione giudiziaria" nel cyberspazio?

Le ragioni principali sono almeno due.

La ragione principale (sostanziale) riguarda il tradizionale divario tra diritto e tecnologia, in cui il diritto è in ritardo rispetto ai progressi tecnologici. L'onere di colmare questa inevitabile inerzia legislativa - a livello nazionale e sovranazionale - ricade pesantemente sulle spalle dei tribunali. Il nuovo contesto fattuale e giuridico creato da Internet ha ulteriormente ampliato questo divario, evidenziando la mancanza di competenze giudiziarie per affrontare gli scenari aperti dalle nuove tecnologie. In questo contesto, l'inerzia politica (non sempre forzata, poiché a volte il potere viene delegato ai tribunali per evitare scelte difficili) ha favorito l'immaginazione giudiziaria nell'era digitale.

La seconda ragione si basa sulla reazione giudiziaria all'approccio basato sulla cyber-anarchia.

Il radicamento della giurisdizione nelle cause relative a Internet è stata la prova migliore che Barlow, nella sua dichiarazione di indipendenza del cyberspazio, si sbagliava quando pensava che i poteri pubblici non potessero regolamentare il cyberspazio.

L'approccio dei tribunali statunitensi ai problemi sollevati dalla natura apparentemente senza confini di Internet è passato da una riconsiderazione dei criteri che avevano stabilito nel tempo per determinare il potere di un tribunale di risolvere le controversie che interessano, direttamente o indirettamente, due o più ordinamenti giuridici.

Per quanto riguarda alcune questioni, come l'esercizio della libertà di parola, la giurisprudenza statunitense ha stabilito i limiti della giurisdizione

personale nelle controversie transfrontaliere sulla base della clausola del *Due Process of Law* del Quattordicesimo Emendamento.

Vale la pena di esaminare questi criteri per capire come i problemi derivanti dalla natura di Internet abbiano trovato soluzioni coerenti con le precedenti sentenze. In *Pennoyer v Neff*[56]la Corte Suprema ha affermato che: "l'autorità di ogni tribunale è necessariamente limitata dai confini territoriali dello Stato in cui è istituito. Qualsiasi tentativo di esercitare l'autorità al di là di tali limiti sarebbe considerato in ogni altro foro [...] un'assunzione illegittima di potere, e sarebbe contrastato come un mero abuso".

Secondo la Corte Suprema degli Stati Uniti nella decisione *Pennoyer c. Neff*, ogni Stato ha giurisdizione "sulle persone e sui beni all'interno del suo territorio"[57].

Questa decisione rifletteva un concetto di giurisdizione personale basato esclusivamente sui confini territoriali, in cui il potere dei tribunali nazionali di giudicare le cause si basa su un collegamento tra lo Stato del foro e il convenuto o i suoi beni.

Questo approccio si è rivelato inadeguato in quanto la crescita del commercio interstatale ha comportato un aumento delle controversie e le nuove tecnologie hanno facilitato la circolazione di persone e merci. In questo modo, un danno poteva essere inflitto e subito in un certo Stato, anche se né il malfattore né la parte lesa vi erano fisicamente presenti.

Pertanto, nella causa *International Shoe Co. c. Washington,*[58] la Corte Suprema, anche se non esplicitamente, ha superato la decisione *Pennoyer* e ha elaborato un test più flessibile che si basa sul raggiungimento di un collegamento minimo tra il convenuto e lo Stato del foro. In particolare, la Corte ha specificato:[59]

"Ma ora che il *capias ad respondendum* ha lasciato il posto alla notifica personale dell'atto di citazione o ad altre forme di notifica, il giusto processo richiede solo che, per sottoporre un convenuto a un giudizio *in personam*, se non è presente nel territorio del foro, abbia determinati contatti minimi con esso tali che il mantenimento della causa non offenda "le nozioni tradizionali di equità e giustizia sostanziale".

Il test del contatto minimo non ha fornito una regola fissa, ma ha richiesto un'indagine fattuale specifica e approfondita in ogni caso in cui fosse in discussione la giurisdizione sul convenuto.

---

56 *Pennoyer v Neff* [1878] 95 U.S. 714.

57 Ibidem.

58 *International Shoe v State of Washington* [1945] 326 U.S. 310.

59 Ibidem, 326.

Inoltre, nella causa *Hanson c. Denckla*[60] la Corte Suprema ha ulteriormente sviluppato il test del contatto minimo, richiedendo al convenuto un atto che costituisca un "utilizzo intenzionale" dei benefici e delle protezioni dello Stato del foro.[61]

Un'importante applicazione di questi criteri nel campo del diritto della responsabilità civile è illustrata nel caso *Calder c. Jones,*[62] dove la Corte ha sviluppato il "test degli effetti". L'attore aveva intentato una causa in California contro due giornalisti, che vivevano e lavoravano in Florida, autori di un articolo presumibilmente diffamatorio pubblicato su un giornale che circolava in California. La Corte Suprema ha ritenuto che la California fosse competente in quanto, date le circostanze, i firmatari dovevano "ragionevolmente prevedere di essere portati in tribunale" per rispondere della veridicità delle affermazioni contenute nel loro articolo. Un individuo leso in California non deve necessariamente recarsi in Florida per chiedere riparazione a persone che, pur rimanendo in Florida, causano consapevolmente il danno in California". [63]

Più in dettaglio, la Corte Suprema ha stabilito un test a tre punte, che si basa sulla consapevolezza del convenuto in merito a tre circostanze: in primo luogo, l'articolo presumibilmente diffamatorio circolava in California; in secondo luogo, l'attore vi risiedeva; infine, le dichiarazioni presumibilmente diffamatorie avrebbero danneggiato la reputazione dell'attore in California.

Come ha influito questo test sulla crescita delle relazioni tramite Internet? La giurisdizione iniziò a essere percepita come una questione chiave, poiché lo sviluppo di Internet implicava che le interazioni sembravano avere luogo ovunque e in nessun luogo.[64]

I tribunali americani, nell'affrontare lo sviluppo dei rapporti giuridici su Internet, hanno cercato di adattare i risultati dei loro sforzi a questo nuovo ambiente, apparentemente senza confini.[65] In questo modo, i giudici hanno preso le distanze dall'approccio di coloro che avevano sostenuto che Internet non poteva essere oggetto di regolamentazione giuridica.

Un ulteriore sviluppo dei criteri sopra elencati è stato fornito nel 1997 nella storica causa *Zippo Manufacturing Co. c. Zippo Dot Com, Inc*.[66] In *Zip-*

---

60 *Hanson v Denckla* [1958] 357 U.S. 235.
61 Ibidem, 253.
62 *Calder v Jones* [1984] 465 U.S. 783.
63 Ibidem 790.
64 JL Goldsmith (1999).
65 U Kohl, Jurisdiction and the Internet. Regulatory Competence over Online Activity(Cambridge, Cambridge University Press 2007).
66 *Zippo Manufacturing Co. v Zippo Dot Com, Inc*. [1997] 952 F. Supp. 1119 (W.D. Pa.).

po, la Corte distrettuale per il distretto occidentale della Pennsylvania ha elaborato il famoso "test della scala mobile", distinguendo i siti web in base a tre livelli di interattività:

La probabilità che la giurisdizione personale possa essere costituzionalmente esercitata è direttamente proporzionale alla natura e alla qualità dell'attività commerciale che un'entità conduce su Internet.

All'inizio, la Corte si è concentrata sui soggetti che gestiscono siti web con lo scopo di concludere affari:

"Se il convenuto stipula contratti con residenti di una giurisdizione straniera che comportano la trasmissione consapevole e ripetuta di file informatici su Internet, la giurisdizione personale è adeguata".

In secondo luogo, il tribunale ha sottolineato che i siti web passivi, a differenza dei primi, sono utilizzati solo per pubblicare informazioni e renderle disponibili in altri paesi, per cui questo tipo di attività non costituisce una solida base per la giurisdizione personale. Infine, la Corte ha dichiarato:[67]

"La via di mezzo è occupata dai siti Web interattivi in cui un utente può scambiare informazioni con il computer ospitante. In questi casi, l'esercizio della giurisdizione è determinato dall'esame del livello di interattività e della natura commerciale dello scambio di informazioni che avviene sul sito Web".

Su queste basi, la Corte distrettuale ha concluso che Zippo Dot Com, una società californiana, era entrata in contatto tramite il suo sito web con i residenti della Pennsylvania allo scopo di fare affari.

Non solo i tribunali americani hanno affrontato problemi di giurisdizione su Internet. Un altro caso emblematico riguardante una richiesta di risarcimento per diffamazione online è stato affrontato nel 2002 dalla High Court of Australia. Nella causa *Dow Jones & Company, Inc. c. Gutnick*[68] l'attore ha presentato una denuncia per diffamazione contro il convenuto, una società di informazioni finanziarie, a causa di un articolo apparso sul suo giornale online. Pochi dei suoi abbonati si trovavano in Australia, ma l'Alta Corte ha deciso il caso, dichiarando:[69] "Se le persone desiderano fare affari in, o addirittura viaggiare, o vivere in, o utilizzare le infrastrutture di diversi Paesi, non possono aspettarsi di essere esentati dal rispetto delle leggi di quei Paesi. Il fatto che la pubblicazione possa avvenire ovunque non significa che non avvenga da nessuna parte".

---

67 Ibidem

68 *Dow Jones & Company, Inc. v Gutnick* [2002] HCA 56.

69 Ibidem, 186.

È noto come la questione del radicamento della giurisdizione sia stata cruciale anche per le Corti europee, come dimostra il caso Google Spagna, per valutare la sovranità digitale europea (e i valori europei) sulle aziende tecnologiche con *server farm* negli Stati Uniti.

Se la migrazione delle idee costituzionali relative al radicamento della giurisdizione è stata un esercizio di successo, non può essere lo stesso per quanto riguarda la disinformazione.

"Internet è un nuovo libero mercato delle idee". Questa è la metafora preferita da coloro che, all'interno del dibattito scientifico e pubblico, ritengono che la questione delle *fake news* non debba essere affrontata dalle autorità pubbliche (e dal diritto pubblico). Come sottolineato da Jacobs, la tutela costituzionale della libertà di parola mira a facilitare la democrazia rappresentativa e a promuovere l'autonomia individuale. Questi valori portano a distinguere tra regolamentazioni governative del discorso e regolamentazioni del discorso che sono neutrali rispetto al contenuto.

Di conseguenza, secondo il paradigma del mercato delle idee, se è vero che secondo il Primo Emendamento "non esiste un'idea falsa" nel mondo materiale,[70] ciò è ancora più vero nella parola digitale, grazie alla maggiore possibilità di esprimere il proprio pensiero. In altre parole, le autorità pubbliche non dovrebbero avere alcun ruolo nell'affrontare i crescenti fenomeni di disinformazione su Internet, perché si suppone che gli utenti abbiano (ottimisticamente) tutti gli strumenti necessari per selezionare le idee più convincenti e le notizie vere, ignorando quelle non convincenti o false.

Questa posizione sottolinea un'espressione di totale fiducia nella capacità di autocorrezione del mercato dell'informazione. Tuttavia, la vera sfida è come tale processo di verifica debba essere condotto secondo i paladini della metafora del libero mercato delle idee, dal momento che per definizione la scarsità di risorse è un limite analogico e non digitale, con la conseguenza che non è necessario tutelare il pluralismo dell'informazione su Internet, le norme giuridiche (e in particolare il diritto pubblico) dovrebbero fare un passo indietro in nome della presunta capacità autocorrettiva del mercato dell'informazione. Così come il mercato economico non conosce test di "validità" dei prodotti, ma lascia che sia la domanda a guidare l'offerta, affidandosi al mercato per distinguere tra prodotti validi e scadenti, il modo migliore per affrontare il fenomeno della disinformazione nel mercato dell'informazione è garantire la più ampia diffusione possibile di tutte le notizie, comprese quelle provenienti da fonti contraddittorie e inaffidabili.

---

70 Gertz v. Welch, 418 U.S. 323 (1974).

Quando la Commissione europea ha deciso di importare dall'humus costituzionale statunitense l'idea del libero mercato delle idee, si è verificato una sorta di effetto di rigetto alla luce del diverso humus costituzionale che caratterizza il costituzionalismo europeo.

L'idea era di investire nell'autoregolamentazione del libero mercato delle idee per quanto riguarda la lotta europea alla disinformazione.

In termini di *policy making* questa idea si è tradotta, nel 2018, nell'adozione di un Codice di Pratica sulla Disinformazione.[71] Si tratta di uno strumento di *soft law* in base al quale le piattaforme si sono impegnate - su base esclusivamente volontaria - ad aderire a una serie di impegni e standard al fine di garantire una migliore qualità dell'informazione. Inoltre, sempre nello stesso anno, la Commissione ha elaborato, di concerto con l'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, un piano d'azione contro la disinformazione[72] che specificava, tra l'altro, che la risposta coordinata dell'Unione doveva basarsi sul miglioramento delle capacità delle istituzioni di individuare, analizzare e smascherare la disinformazione, sul rafforzamento delle risposte coordinate e congiunte alla disinformazione, sulla mobilitazione del settore privato per affrontare la disinformazione e sul sostegno alle iniziative di sensibilizzazione e di miglioramento della resilienza della società.

La strategia adottata in questa seconda fase ha perseguito un approccio di autoregolamentazione in questo settore, in un certo senso vicino al modello statunitense e alla metafora, tipica di quel modello, del "libero mercato delle idee"; tuttavia, si è presto rivelata insoddisfacente. In particolare, il sostanziale fallimento del Codice di condotta è stato messo in forte evidenza soprattutto a seguito dello scoppio della pandemia nel 2020[73] e dell'invasione russa dell'Ucraina nel 2022. Inoltre, quasi parallelamente all'adozione di queste strategie, alcuni Stati nazionali hanno scelto di perseguire (o, come

---

71 Codice di buone pratiche dell'UE sulla disinformazione, https://ec.europa.eu/newsroom/dae/redirection/document/87534, 20 settembre 2018.

72 Comunicazione congiunta JOIN(2018)36 della Commissione e dell'Alto rappresentante per gli affari esteri e la politica di sicurezza del 5 dicembre 2018 al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni sul piano d'azione contro la disinformazione.

73 Così, in particolare, Commissione europea, "Assessment of Practice on Disinformation - Achievements and areas for further improvement", SWD(2020)180, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=69212, 10 settembre 2020, p. 19: *"[T]this overall assessment highlights that ... the Code should be further improved in several areas by providing commonly-shared definitions, clearer procedures, more precise commitments as well as transparent key performance indicators and appropriate monitoring, all taking into account applicable regulatory frameworks. Si dovrebbero inoltre compiere ulteriori sforzi per ampliare la partecipazione ad altre parti interessate, in particolare al settore pubblicitario*".

vedremo più avanti in relazione all'Italia, hanno tentato di perseguire) opzioni di più ampia portata.

Il pioniere in questo campo è senza dubbio la legge tedesca sull'applicazione della rete (*Netzwerkdurchsetzungsgesetz*, NetzDG),[74] il cui obiettivo dichiarato è quello di combattere la diffusione di contenuti illegali online, tra cui numerosi casi di incitamento all'odio e di disinformazione.[75] La NetzDG impone una serie di obblighi agli operatori dei *social network* e delle piattaforme di condivisione video con l'obiettivo, in primo luogo, di ottenere una maggiore trasparenza per quanto riguarda le politiche e le pratiche di moderazione dei contenuti illegali e, in secondo luogo, di mettere in atto meccanismi di "*notice-and-take-down*". Si tratta, in pratica, dell'adozione di procedure che consentano agli utenti di segnalare ai provider la presenza di contenuti illeciti sulle piattaforme da loro gestite. In caso di segnalazione, il *provider* è tenuto a rispondere e, se il contenuto viola effettivamente una disposizione del Codice penale tedesco, a rimuoverlo entro un breve periodo di tempo. I *provider* sono passibili di multe salate se non rispettano sistematicamente questi obblighi.[76]

---

74 *Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken*. Sulla legge, si vedono tra gli altri Victor Claussen (2018*), Fighting hate speech and fake news*. Il *Network Enforcement Act* (NetzDG) *in Germania nel contesto della legislazione europea*, Rivista di diritto dei media", 3, pp. 110-136; Thomas Wischmeyer, 'What Is Illegal Offline Is Also Illegal Online: The German Network Enforcement Act 2017', in Bilyana Petkova e Tuomas Ojanen (a cura di), *Fundamental Rights Protection Online*: The Future Regulation of Intermediaries, Cheltenham, Edward Elgar, 2020, pp. 28-56; Nannerel Fiano, "Il linguaggio dell'odio in Germania: *Tra Wehrhafte Demokratie e Netzwerkdurchsetzungsgesetz*", in Marilia D'Amico e Cecilia Siccardi (a cura di), *La costituzione non odia: Conoscere, prevenire e contrastare l'hate speech online*, Torino, Giappichelli, 2021, pp. 155-165; Mathias Hong (2022), "Regulating Hate Speech and Disinfomration Online While Protecting Freedom of Speech as an Equal and Positive Right - Comparing Germany, Europe and the United States", *Journal of Media Law*, 14, pp. 76-96.

75 In realtà la legge non introduce una specifica definizione di disinformazione (né di hate speech), ma si limita a fare un rimando a una serie di fattispecie penali già individuate nel codice penale federale. Manca dunque il riconoscimento a livello legislativo di un'autonoma identità giuridica del fenomeno della disinformazione.

76 Tale disciplina è stata oggetto di numerose critiche, provenienti non solo dai gestori delle piattaforme stesse, ma anche da attivisti e accademici che hanno sottolineato i rischi inerenti a tale legislazione in termini di tutela della libertà di espressione. In effetti, l'imposizione di obblighi di moderazione di contenuti illeciti potrebbe spingere le piattaforme digitali a porre in essere forme di "censura collaterale" potenzialmente dannose per i diritti degli internauti stessi. Si vedano, tra gli altri, Heidi Tworek e Paddy Leerssen, "An Analysis of Germany's NetzDG Law", www.ivir.nl/publicaties/download/NetzDG_Tworek_Leerssen_April_2019.pdf, 15 aprile 2019; Isabelle Canaan (2022), "NetzDG and the German Precedent for Authoritarian Creep and Authoritarian Learning", Columbia Journal of European Law, 28, pp. 101-133. Sul concetto di "censura collaterale", vedi Jack M. Balkin (1999), "Free Speech and Hostile Environments", Columbia Law Review, 99(8), pp. 2295-2320, p. 2298.

D'altra parte, nel 2018 la Francia ha emanato diverse misure legislative per combattere la "manipolazione dell'informazione"[77], con particolare attenzione al suo impatto sulle elezioni. Queste iniziative sono state inoltre avviate sulla scia delle *fake news* che hanno funestato la campagna elettorale presidenziale del 2017, anche se non hanno avuto effetti significativi sul risultato. La legislazione specifica applicabile durante le elezioni impone innanzitutto una serie di requisiti di trasparenza aggiuntivi, tra cui l'obbligo di pubblicare la fonte e l'importo di qualsiasi pagamento ricevuto dalle piattaforme. In secondo luogo, prevede una procedura speciale dinanzi ai tribunali e una procedura amministrativa dinanzi all'*Authorité de régulation de la communication audiovisuelle et numérique* (ARCOM), con l'obiettivo di bloccare la diffusione della disinformazione attraverso i servizi pubblici di comunicazione online e di impedire la trasmissione alla radio e alla televisione di "false informazioni" provenienti da Paesi terzi.[78]

Alla luce della necessità di evitare i fallimenti delle strategie passate (tra cui, in particolare, il Codice di condotta del 2018), garantendo al contempo un approccio armonizzato e unitario a livello sovranazionale, sembra essere iniziata di recente una "terza fase" nella lotta alla disinformazione in Europa. Essa è stata caratterizzata in particolare dall'adozione di una legislazione di maggiore portata e impatto a livello dell'UE.

Inoltre, il primo e più significativo sviluppo in questo contesto ha riguardato il Codice di condotta sulla disinformazione e il suo rapporto con la nuova legge sui servizi digitali (DSA). Infatti, come già osservato nel capitolo 2, dopo che nel 2018 il Codice si è rivelato inefficace, la Commissione ha iniziato a lavorare su due binari paralleli: in primo luogo una profonda revisione del Codice[79] e in secondo luogo la sua trasformazione da strumento di

---

77 *Loi organique n. 2018-1201 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information e Loi n. 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information*.

78 La nuova disciplina francese è stata peraltro oggetto di alcune questioni preliminari di costituzionalità: uno dei problemi più rilevanti concerneva, in particolare, l'identificazione di ciò che possa essere considerato effettivamente "falso". In tal senso, il Conseil Constitutionnel, attraverso una sentenza interpretativa di rigetto, ha affermato, come condizione per la validità costituzionale della legge, la necessità che la falsità delle informazioni possa essere dimostrata in modo oggettivo, nonché la necessità che l'action judiciaire en référée non investa semplici opinioni, parodie, imprecisioni parziali o esagerazioni; inoltre, il carattere fuorviante dei contenuti disinformativi e l'impatto sulle procedure elettorali devono essere manifesti. Vedi Cons. Cost., sentenza n. 2018-773 DC del 20 dicembre 2018, para. 21.

79 Vedi, in tal senso, Comunicazione COM/2020/790, cit.; Comunicazione COM/2021/262 della Commissione del 26 maggio 2021 al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni sugli orientamenti della Commissione europea sul rafforzamento del codice di buone pratiche sulla disinformazione, 26 maggio 2021, COM(2021)262.

autoregolamentazione a strumento di coregolamentazione.

Per quanto riguarda il secondo aspetto, gli articoli 34 e 35 della DSA impongono ai fornitori di piattaforme *online* e di motori di ricerca *online* di grandi dimensioni l'obbligo di mettere in atto meccanismi per la valutazione e l'attenuazione dei rischi sistemici che riguardano, tra l'altro, "qualsiasi effetto negativo effettivo o prevedibile sul discorso civico e sui processi elettorali". Questa clausola affronta chiaramente il problema della disinformazione. Allo stesso tempo, l'articolo 45 delle DSA prevede la possibilità di redigere codici di condotta, generalmente su iniziativa della Commissione, che prevedano, tra l'altro, l'adozione di specifiche misure di mitigazione del rischio, nonché un quadro di rendicontazione periodica sulle misure adottate e sui loro risultati.[80] Come menzionato nel capitolo 2, se da un lato questi codici consentono all'Unione di mettere in atto standard comuni adeguati, e quindi di raggiungere gli obiettivi in modo più efficace, dall'altro assicurano una maggiore certezza per i fornitori per quanto riguarda le misure di mitigazione del rischio che devono essere attuate.

Questo spiega il ruolo preminente che il nuovo codice del 2022 ha svolto in quanto, tenendo conto in particolare delle regole stabilite dalla DSA sui codici di condotta, è stato adottato specificamente con l'obiettivo centrale di operare non solo come strumento interpretativo ma anche come standard comune per la lotta alla disinformazione ai sensi degli articoli 34 e 35[81]. Pertanto, dal Codice di condotta rafforzato adottato nel 2022 emerge chiaramente che l'Unione è passata da una strategia di stretta autoregolamentazione a una strategia di coregolamentazione. L'adesione agli impegni previsti dal Codice (che sono molto più ampi di quelli contenuti nel suo predecessore del 2018) è ora sostenuta dalla nuova legge sui servizi digitali e come tale - pur non essendo obbligatoria - è almeno fortemente caldeggiata.

Tuttavia, gli aspetti innovativi della nuova fase dell'approccio europeo alla disinformazione non si limitano solo al superamento del primato dell'autoregolamentazione a favore di un intervento più dall'alto verso il basso.

Il passaggio da un'autoregolamentazione a una coregolamentazione, che è stato descritto a proposito dei nuovi sviluppi (basati sulla *hard law*) nella governance dell'informazione *online*, è stato descritto come una sorta di "rivoluzione".

Più precisamente, negli ultimi anni, la questione fondamentale dell'informazione *online* e del suo impatto sui valori e sui processi democratici in-

80 DSA, art. 45, para. 2.

81 Si veda, tra gli altri, Matteo Monti (2022), *"Lo strengthened Code of Practice on Disinformation*: un'altra pietra della nuova fortezza digitale europea?". *Rivista di diritto dei media*, 2, 2022, pp. 317-321.

terni ha portato all'adozione di ulteriori misure legislative volte a promuovere un ecosistema digitale commisurato ai requisiti "costituzionali" dell'UE. Uno sviluppo particolarmente importante si è avuto con l'approvazione, nei primi mesi del 2024 e quindi poco prima delle elezioni del Parlamento europeo, di due regolamenti volti a disciplinare meglio la diffusione del giornalismo *online* e della pubblicità politica *online*. Si tratta in particolare del Regolamento (UE) 2024/900 "sulla trasparenza e l'orientamento della pubblicità politica"[82] e del Regolamento (UE) 2024/1083 sulla libertà dei media - quest'ultimo comunemente indicato anche come *European Media Freedom Act (EMFA)*. [83]

L'obiettivo finale del Regolamento (UE) 2024/900 era quello di introdurre norme uniformi a livello europeo per disciplinare la diffusione e la distribuzione della pubblicità politica, anche e soprattutto alla luce della natura frammentaria della legislazione nazionale precedentemente applicabile.[84] Il preambolo del nuovo Regolamento mostra ancora una volta che esso aspira a trovare un equilibrio tra valori intrinsecamente costituzionali e democratici. Lo fa innanzitutto garantendo un elevato grado di trasparenza per quanto riguarda la distribuzione della pubblicità politica, assicurando al contempo che "la fornitura di pubblicità politica avvenga nel pieno rispetto dei diritti fondamentali"[85], nonché dei requisiti relativi alla promozione del mercato digitale e soprattutto della necessità di tutelare gli interessi dei fornitori di servizi di pubblicità politica - in particolare "le micro, piccole e medie imprese, che spesso non hanno le risorse per assorbire o trasferire gli elevati costi di conformità connessi alla preparazione, al collocamento, alla promozione, alla pubblicazione, alla consegna o alla diffusione di pubblicità politica in più di uno Stato membro". [86]

Come suggerisce il titolo, il Regolamento (UE) 2024/900 si concentra specificamente sulle "tecniche di *targeting*", definite come "tecniche utilizzate per indirizzare una pubblicità politica solo a una persona o a un gruppo di persone specifiche o per escluderle, di solito con contenuti personalizzati,

---

82 Regolamento (UE) 2024/900 del Parlamento europeo e del Consiglio, del 13 marzo 2024, relativo alla trasparenza e al targeting della pubblicità politica.

83 Regolamento (UE) 2024/1083 del Parlamento europeo e del Consiglio, dell'11 aprile 2024, che istituisce un quadro comune per i servizi di media nell'ambito del mercato interno e che modifica la direttiva 2010/13/UE (regolamento europeo sulla libertà dei media). Si veda, in particolare, Oreste Pollicino e Federica Paolucci (2024), "Unveiling the Digital Side of Journalism: Exploring the European Media Freedom Act's Opportunities and Challenges", La Revue des Juristes de Sciences Po, 1.

84 Regolamento (UE) 2024/900, cit., considerando 9.

85 Ibidem, considerando 5.

86 Ibidem, considerando 10.

sulla base del trattamento dei dati personali".[87] È chiaro che questa nuova legislazione opera all›intersezione tra la governance dei dati e la *governance* dell'informazione *online*, modificando le norme che regolano il ricorso alle tecniche di profilazione degli utenti ai fini della distribuzione di contenuti, nonché la struttura stessa dell'ecosistema digitale *online*. Il Regolamento sottolinea come l'utilizzo di queste tipologie di sistemi decisionali automatizzati sia associato al rischio di effetti collaterali significativi in termini di tutela dei diritti fondamentali e dell'autodeterminazione individuale, in particolare quando sono coinvolte "categorie particolari di dati" ai sensi dell'articolo 9, paragrafo 1, del GDPR:[88]

Tale trattamento di dati personali ha effetti specifici e dannosi sui diritti e le libertà fondamentali delle persone, quali il trattamento equo e paritario, il non essere manipolati, il ricevere informazioni obiettive, il formarsi un'opinione, il prendere decisioni politiche e l'esercitare il diritto di voto. Inoltre, ha un impatto negativo sul processo democratico, in quanto porta alla frammentazione del dibattito pubblico su importanti questioni sociali, alla diffusione selettiva e, in ultima analisi, alla manipolazione dell'elettorato. Aumenta inoltre il rischio di diffusione di manipolazioni dell'informazione e di interferenze straniere.[89]

Non sorprende quindi che il regolamento sottoponga l'uso di queste tecniche a restrizioni significative. Esso richiede, tra l'altro, che l'unica base giuridica valida per il trattamento dei dati a fini di *targeting* sia il consenso esplicito della persona interessata. Inoltre, vieta espressamente che queste tecniche si trasformino in forme di profilazione che utilizzano categorie particolari di dati ai sensi dell'articolo 9, paragrafo 1, del GDPR.[90] I legislatori erano chiaramente preoccupati della possibilità di un'indebita interferenza nella stessa "libertà cognitiva"[91] degli utenti di Internet, che avrebbe potuto avere ramificazioni significative non solo per i diritti individuali ma anche, nel complesso, per i processi decisionali democratici e politici.

Anche il secondo strumento legislativo menzionato, lo *European Media Freedom Act*, è pienamente coerente con la strategia europea di promozione del dibattito online, che si fonda sul pluralismo, su una maggiore tra-

87 Ibidem, art. 3(11).

88 Dispone l'art. 9 del GDPR: "È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona".

89 Regolamento (UE) 2024/900, cit., considerando 74.

90 Ibidem, art. 18(1).

91 Vedi, sul tema, Oreste Pollicino (2021), "Costituzionalismo, privacy e neurodiritti", *Rivista di diritto dei media*, 2, pp. 9-17.

sparenza e su una migliore qualità delle informazioni trasmesse attraverso le infrastrutture digitali. I cambiamenti introdotti dal regolamento, in particolare per quanto riguarda l'obiettivo di combattere la disinformazione *online*, saranno esaminati in modo più approfondito nel capitolo 4. A questo punto, sembra opportuno che l'automazione e l'uso di sistemi decisionali automatizzati svolgano un ruolo particolarmente importante anche all'interno dell'AEM, in particolare per quanto riguarda la necessità di stabilire garanzie sufficienti per proteggere gli utenti di fronte a un'indebita interferenza nella loro libertà personale durante la ricerca di informazioni.

Di conseguenza, l'EMFA ha previsto la creazione di uno specifico "diritto alla personalizzazione dell'offerta mediatica", ossia il diritto di modificare facilmente la configurazione, comprese le impostazioni predefinite, di qualsiasi dispositivo o interfaccia utente che controlla o gestisce l'accesso e l'uso dei servizi di media che forniscono programmi, al fine di personalizzare l'offerta mediatica in base ai propri interessi o preferenze, nel rispetto del diritto dell'Unione.[92]

Il quadro giuridico stabilito dai due nuovi regolamenti adottati nel 2024 sembra confermare ancora una volta l'aspirazione a portare l'Unione in una nuova fase legislativa, definita "costituzionalismo digitale". Questo approccio cerca di infondere nel diritto principi e valori democratici e costituzionali, tra cui il diritto a ottenere un'informazione pluralista e di qualità, il diritto all'autodeterminazione nel processo decisionale e il diritto a libere elezioni nell'ambito di una nuova società algoritmica. Anche in questo caso, infatti, si è cercato di trovare un giusto equilibrio tra l'interesse al pieno sviluppo delle nuove tecnologie - che peraltro hanno il potenziale per agire come strumenti straordinariamente potenti per far progredire il dibattito democratico - e la necessità di contenere i rischi associati all'emergere degli algoritmi e degli attori digitali privati come nuovi protagonisti della scena globale.

Un altro aspetto particolarmente significativo riguarda la promozione attiva dei valori del pluralismo informativo e il tentativo di garantire un miglioramento complessivo della qualità della comunicazione mediatica. Questo obiettivo è perseguito in modo specifico dal nuovo Regolamento (UE) 2024/1083 approvato nell'aprile 2024 sulla libertà dei media (*European Media Freedom Act, EMFA*),[93] di cui si è già parlato nel capitolo 2.

---

92 EMFA, cit., art. 20(1).

93 Regolamento (UE) 2024/1083 del Parlamento europeo e del Consiglio, dell'11 aprile 2024, che istituisce un quadro comune per i servizi di media nell'ambito del mercato interno e che modifica la direttiva 2010/13/UE (regolamento europeo sulla libertà dei media). Si veda sul punto, in particolare, Oreste Pollicino e Federica Paolucci (2024), "Unveiling the Digital Side of Journalism: Exploring the European Media Freedom Act's Opportunities and Challenges", La Revue des Juristes de Sciences Po, 1.

Come già indicato nella relazione sulla proposta,[94] l'obiettivo principale del nuovo regolamento è quello di sostenere il ruolo fondamentale svolto dai media indipendenti all'interno della società civile, nella misura in cui i media contribuiscono a formare l'opinione pubblica, fornendo ai cittadini una varietà di opzioni e informazioni affidabili. In quest'ottica, l'obiettivo dichiarato del regolamento è quello di garantire il pluralismo e l'indipendenza dei media, nonché un giornalismo pluralista e indipendente. Ad esempio, l'articolo 4 introduce importanti diritti e garanzie che possono essere esercitati dai fornitori di servizi di media nei confronti degli Stati membri. L'articolo 5 stabilisce alcune garanzie per proteggere l'indipendenza dei fornitori di servizi di media pubblici. D'altra parte, l'articolo 6 impone una serie di obblighi di trasparenza ai fornitori di servizi di media in generale (soprattutto per quanto riguarda l'identità dei proprietari e degli enti finanziatori), e in particolare ai servizi di media che forniscono contenuti di notizie e attualità (per adottare misure adeguate a garantire l'indipendenza delle singole decisioni editoriali).

Inoltre, l'*EMFA* riconosce l'importanza dei media digitali nel mondo contemporaneo, nonché l'impatto che i modelli commerciali delle piattaforme *online* hanno in termini di contributo alla crescente polarizzazione e alla disinformazione *online*. È inoltre consapevole del rischio per l'indipendenza dei media causato dal finanziamento e/o dal controllo di Paesi terzi.[95] Per questo motivo, l'*EMFA* stabilisce regole interessanti per disciplinare le relazioni tra i fornitori di servizi mediatici e i fornitori di Very Large Online Platforms (VLOP), che cercano di integrare il Digital Service Act (DSA) con un riferimento specifico al settore giornalistico.

In particolare, i fornitori di piattaforme *online* di grandi dimensioni devono incorporare una funzione che consenta ai fornitori di servizi mediatici

---

94 Proposta di Regolamento del Parlamento europeo e del Consiglio che istituisce un quadro comune per i servizi di media nell'ambito del mercato interno e che modifica la direttiva 2010/13/UE, COM/2022/457.

95 Così EMFA, considerando 3-4: "Nello spazio dei media digitali i cittadini e le imprese accedono e consumano contenuti mediatici e servizi di media, che sono immediatamente accessibili sui loro dispositivi personali, in un contesto sempre più transfrontaliero ... Il mercato interno dei servizi di media però non è sufficientemente integrato ed è soggetto a una serie di fallimenti del mercato sempre più numerosi a causa della digitalizzazione. In primo luogo, le piattaforme online globali fungono da punti di accesso ai contenuti mediatici, con determinati modelli commerciali che tengono a basarsi sulla disintermediazione dell'accesso ai servizi di media e ad amplificare la polarizzazione dei contenuti e la disinformazione ... In terzo luogo, il buon funzionamento del mercato interno dei servizi di media è compromesso da fornitori, compresi quelli controllati da determinati paesi terzi, che si dedicano in modo sistematico ad attività di disinformazione, o manipolazione delle informazioni e ingerenze, e sfruttano le libertà del mercato interno a fini abusivi, ostacolando in tal modo il corretto funzionamento delle dinamiche di mercato".

di: identificarsi come tali; dichiarare di essere editorialmente indipendenti dagli Stati membri e dai Paesi terzi; dichiarare di essere soggetti a requisiti normativi per l'esercizio della responsabilità editoriale in uno o più Stati membri o di aderire a un meccanismo di coregolamentazione o autoregolamentazione "ampiamente riconosciuto e accettato nel settore dei media pertinente in uno o più Stati membri"; e "dichiarare di non fornire contenuti generati da sistemi di intelligenza artificiale senza sottoporli a revisione umana o controllo editoriale"[96]. (Una volta che questa dichiarazione è stata fatta e il fornitore di servizi di media è stato riconosciuto come "professionale", sarà trattato in modo diverso per quanto riguarda l'attività di moderazione sulla piattaforma. Ciò comporta, ad esempio, la notifica preventiva di qualsiasi decisione di sospendere la fornitura di servizi di intermediazione).

D'altra parte, l'*EMFA* prevede anche la possibilità di avviare un "dialogo strutturato" tra le parti interessate, il Comitato europeo per i servizi media e la società civile. L'obiettivo di questo dialogo è garantire uno scambio di esperienze e sviluppare le migliori pratiche nell'applicazione del meccanismo di moderazione e nella promozione del pluralismo dei media sulle piattaforme *online*. La necessità di proteggere la società da contenuti dannosi è specificamente menzionata, compresa la "disinformazione e la manipolazione e interferenza dell'informazione straniera".[97]

La legislazione che ne deriva sembra quindi essenzialmente incentivare forme di cooperazione tra piattaforme *online*, autorità europee e fornitori di servizi mediatici. L'obiettivo specifico di fondo è quello di tutelare la diffusione di un'informazione indipendente, pluralista e corretta, di contrastare i contenuti falsi o inquinanti provenienti anche (sebbene non esclusivamente) da Paesi stranieri e, infine, di rafforzare l'autodeterminazione degli utenti della rete in relazione all'informazione (e al processo decisionale).

Infine, un terzo aspetto di particolare rilevanza riguarda il riconoscimento a livello europeo della stretta interconnessione tra disinformazione e IA, nonché dell'impatto che tale interconnessione ha sul corretto funzionamento dei processi democratici interni. Questo riconoscimento riflette la rinnovata consapevolezza (descritta sopra nel capitolo 2) del cambiamento di paradigma che i recenti sviluppi relativi all'intelligenza artificiale - e in particolare i progressi nell'apprendimento automatico, nell'IA generativa, negli LLM ecc. - hanno portato sulla scena tecnologica e sociale mondiale.

In generale, come si è cercato di dimostrare, è chiaro che il nuovo approccio dell'UE cerca di affrontare su più fronti i vari aspetti della disinfor-

96 EMFA, art. 17.
97 Ibidem, art. 19(1).

mazione. Ciò comporta, come si vedrà nel prossimo capitolo, un'attenzione particolare al modo in cui la disinformazione interagisce con lo sviluppo e la diffusione dell'IA, da un lato, e con le conseguenze per i media (e, per estensione, per i processi democratici), dall'altro. Inoltre, questo approccio su più fronti sembra essere caratterizzato da una forte tendenza da parte dell'UE a superare la strategia puramente diplomatica e comunicativa della prima fase e l'approccio di autoregolamentazione della seconda, per passare a una forma di co-regolamentazione della governance della disinformazione, o addirittura, in alcuni casi, a una vera e propria *hard law*.

SISTEMI E MODELLI DI IA PER IL RAFFORZAMENTO DELLA CYBERSICUREZZA NAZIONALE. CONSERVARE LE PROVE CONTRASTANDO GLI ATTACCHI INFORMATICI

Nunzia Ciardi
Vice Direttore dell'Agenzia per la Cybersicurezza Nazionale

L'intelligenza artificiale, e, in particolare, quella generativa, pur essendo una manifestazione relativamente recente di una tecnologia esistente da decenni, si inserisce in uno scenario eterogeneo e complesso, sollevando questioni fondamentali riguardo ai concetti di sovranità, giurisdizione e territorialità. La sua introduzione ha il potenziale di destabilizzare ulteriormente i paradigmi esistenti, rendendo ancora più urgente l'esigenza di un ripensamento giuridico e politico. Queste tecnologie emergenti stanno infatti modificando profondamente il contesto normativo e politico globale, sfidando l'efficacia degli strumenti normativi tradizionali e richiedendo un approccio interdisciplinare per affrontare le loro implicazioni socioeconomiche e geopolitiche.

L'intelligenza artificiale rappresenta, dunque, un elemento chiave nel plasmare il futuro equilibrio geopolitico, favorendo le nazioni che saranno in grado di governarla con efficienza e lungimiranza. Non sorprende, pertanto, che le principali potenze globali, come Stati Uniti, Cina, Arabia Saudita e diverse altre nazioni, stiano investendo ingenti risorse nello sviluppo e nell'applicazione dell'IA. La dimensione degli investimenti in questo campo non riguarda solo la costruzione di capacità tecnologiche, ma anche la creazione di un ecosistema integrato, che supporti l'innovazione e il controllo di questa tecnologia strategica.

L'intelligenza artificiale, di per sé, non è una tecnologia radicalmente innovativa: il suo potenziale risiede nella straordinaria quantità di dati oggi disponibili e nella crescente capacità computazionale. La disponibilità di questi due fattori si sta espandendo a ritmi vertiginosi, sollevando la questione di chi effettivamente detenga la proprietà dei dati e, di conseguenza, il controllo di fatto degli algoritmi che su questi ultimi vengono "addestrati". Tali dati, spesso, non appartengono a singoli Stati, organizzazioni o società, introducendo così importanti implicazioni di carattere geopolitico, economico e sociale. La capacità di raccogliere e utilizzare questi strumenti determina infatti un significativo vantaggio competitivo a livello internazionale, aumentando il divario tra i Paesi che dispongono delle risorse (dati e potenza computaziona-

le *in primis*, ma anche talenti) per sfruttare tali tecnologie e quelli che, invece, non possedendole, ne sono esclusi.

L'IA si fonda, dunque, su due "pilastri": la disponibilità dei c.d. "*big data*" e una capacità computazionale avanzata, fattori che, come abbiamo detto, stanno rapidamente assumendo una rilevanza centrale nel panorama globale. Basti pensare che, nel 2024, il numero di utenti di Internet ha raggiunto quasi i 5,5 miliardi, corrispondenti a circa due terzi della popolazione mondiale. Inoltre, il numero di dispositivi connessi ha superato gli 8 miliardi, contribuendo a generare un volume di dati fondamentale per l'addestramento dei modelli di IA. La proliferazione dei dispositivi connessi e la loro crescente capacità di interagire tra loro senza intervento umano stanno creando un ecosistema digitale altamente complesso, in cui la quantità e la qualità dei dati disponibili sono destinate a crescere esponenzialmente.

Un simile scenario pone sfide significative alla sicurezza nazionale e internazionale. La capacità dell'intelligenza artificiale di elaborare enormi quantità di dati in tempi brevissimi la rende una straordinaria opportunità, ma anche un potenziale vettore o "facilitatore" di minacce molto serie. Un esempio eclatante è quello dei c.d. *deep fake*: la capacità di generare contenuti video falsi, ma altamente realistici, ha già dimostrato la sua pericolosità: oltre alle sempre più insidiose e verosimili truffe, pensiamo ai potenziali impatti politici, economici o sulla pubblica sicurezza che potrebbero derivare dalla diffusione, ad esempio, di false dichiarazioni da parte una figura politica o di governo, arrivando a mettere a rischio la stabilità politica e la fiducia nelle istituzioni.

Anche minacce apparentemente più ordinarie, come il *phishing*, stanno diventando sempre più sofisticate grazie all'uso malevolo dell'IA, divenendo quasi indistinguibili da comunicazioni lecite e reali. Questi attacchi non solo sono in grado di ingannare individui comuni, ma anche di colpire le organizzazioni più strutturate, con conseguenze potenzialmente devastanti. Inoltre, algoritmi avanzati possono essere impiegati per analizzare codici alla ricerca di vulnerabilità nei sistemi informatici, automatizzando la ricerca dei bersagli. I *malware* dotati di capacità di "auto-addestramento" rappresentano un ulteriore pericolo: una volta introdotti in un sistema, sono in grado di migliorare continuamente le proprie strategie di evasione e infiltrazione. Tali considerazioni divengono ancor più attuali e rilevanti quando ci si rivolge ad infrastrutture critiche o sensibili, come quelle sanitarie: un attacco ai danni anche di una singola azienda sanitaria locale – da cui dipendono diverse strutture, ospedali e presidi sanitari –, infatti, può avere impatti notevoli, con effetti a cascata che vanno ben oltre il singolo soggetto colpito.

Un ulteriore aspetto, che non va trascurato, è che l'IA stessa, in quanto

algoritmo, è attaccabile. Lo si può fare in vari modi: "avvelenando", ad esempio, i dati stessi su cui questa viene addestrata. Questo fenomeno è estremamente insidioso, poiché comporta il rischio (di per sé già intrinseco all'IA stessa, in quanto i suoi processi decisionali interni sono caratterizzati da "opacità") di introdurre risultati inattesi, fuorvianti o persino pericolosi, compromettendone irrimediabilmente l'affidabilità: se i dati che alimentano gli algoritmi sono alterati, anche le applicazioni che si basano su di essi saranno alterate, con conseguenze significative sugli *output* prodotti da queste tecnologie che, va ricordato, sono e saranno sempre più presenti e pervasive.

In tale contesto, il concetto di resilienza diventa cruciale: come la madre di Winnicott, noto psicoanalista e pediatra britannico del secolo scorso, la sicurezza perfetta "non esiste", esiste quella "sufficientemente buona". Anche con difese altamente sofisticate, esiste sempre la possibilità che una minaccia passi inosservata o che un attacco particolarmente elaborato riesca a superare le misure di protezione. L'importante, e qui entra in gioco la resilienza, è sviluppare la capacità di rialzarsi, riprendersi e reagire dopo il colpo subito, ripristinando l'operatività dei sistemi e assicurando la continuità dei servizi nel più breve tempo possibile, minimizzandone le conseguenze negative.

Si pensi, di nuovo, all'esempio del settore sanitario: un attacco andato a buon fine, in questi casi, potrebbe comportare l'interruzione di servizi essenziali e terapie salvavita, bloccando pronto soccorso, ambulanze e sale operatorie. Ed è un fenomeno che non riguarda soltanto l'Italia, ma tutti i Paesi più avanzati. Per questo motivo, è essenziale implementare misure che riducano al minimo i danni causati da un attacco e garantire il più rapido ripristino dei servizi.

In quest'ottica, l'Agenzia per la Cybersicurezza Nazionale (ACN) ha adottato il concetto di resilienza come principio guida, con l'obiettivo di garantire il ripristino tempestivo dei sistemi compromessi e proteggere, così, anche la sicurezza nazionale nello spazio cibernetico. Il che si traduce, concretamente, in pratiche operative che vanno dalla progettazione di sistemi più robusti alla formazione di personale specializzato, fino alla creazione di protocolli di risposta coordinata che coinvolgano sia il settore pubblico che quello privato.

La resilienza cibernetica ha recentemente ricevuto un importante riconoscimento giuridico attraverso la Legge n. 90/2024, che, oltre a disciplinare più diffusamente i rapporti operativi e i raccordi informativi tra ACN, Autorità Giudiziaria e Polizia Giudiziaria, ha introdotto opportuni meccanismi di bilanciamento tra le esigenze investigative e quelle di resilienza nazionale, funzionali ad assicurare l'efficace e tempestivo svolgimento delle attività di ripristino, l'assicurazione delle fonti di prova e il coordinamento del Procuratore Nazionale Antimafia e Antiterrorismo (PNAA).

In particolare, la norma ha previsto che l'Agenzia debba informare il PNAA della notizia di un attacco ai danni di determinati sistemi informatici o telematici e, in ogni caso, quando risulti interessato un soggetto del Perimetro di Sicureza Nazionale , NIS o Telco, e che il Pubblico Ministero (PM) informi l'ACN quando acquisisce notizia di alcuni gravi reati informatici, assicurando anche il raccordo informativo con il CNAIPIC. Inoltre, la medesima legge ha introdotto specifici meccanismi di bilanciamento tra indagini e resilienza, prevedendo: da un lato, che il PM impartisca le disposizioni necessarie ad assicurare che gli accertamenti urgenti siano compiuti tenendo conto delle attività svolte dall'Agenzia a fini di resilienza; dall'altro, che, per evitare un grave pregiudizio per il corso delle indagini, il PM possa disporre il differimento delle attività di resilienza con provvedimento motivato.

Un caso emblematico è stato l'arresto di un giovane *hacker*, resosi responsabile di un attacco ai sistemi della Giustizia italiana: grazie alla collaborazione tra l'ACN, la DNA, le Procure inquirenti e la Polizia Postale, è stato possibile mettere in sicurezza i sistemi compromessi senza inficiare le indagini in corso, assicurando così la continuità dei servizi critici nel rispetto delle esigenze investigative. Questa esperienza ha dimostrato l'efficacia di un approccio coordinato e sinergico alla gestione degli incidenti di sicurezza – che sono anche reati, ma non solo –, evidenziando l'importanza della cooperazione tra le diverse istituzioni coinvolte.

Il dominio cyber è un dominio diverso dagli altri: è trasversale, sfaccettato e mutevole. È un dominio nel quale siamo immersi tutti in prima persona. Di conseguenza, bisogna riconoscere che la resilienza e la sicurezza cyber poggiano sulle spalle di ciascuno di noi: su ogni singola azienda, su ogni singola istituzione, su ogni singolo cittadino. Solo attraverso un approccio olistico, dunque, si riuscirà, se non ad eliminarlo, a ridurre il rischio cyber a un livello quantomeno "fisiologico".

Un tale approccio, per realizzarsi compiutamente, poggia su un elemento fondamentale: la cultura. Possiamo spendere milioni di euro per mettere in sicurezza i sistemi, ma se un dipendente non adotta tutte le cautele necessarie e, ad esempio, durante lo *smart working*, collega il computer di servizio alla rete domestica senza precauzioni, ogni investimento rischia di rivelarsi futile. Per una mancanza di cultura della sicurezza, viene così vanificato lo sforzo complessivo di un'intera organizzazione. È, pertanto, fondamentale investire sulla formazione e sulla diffusione della consapevolezza dei rischi cyber a tutti i livelli e in tutti i settori, soprattutto con riguardo alle sfide e alle opportunità offerte dalle nuove tecnologie in un mondo sempre più digitalizzato.

In conclusione, tornando sul tema dell'intelligenza artificiale, emblematico dell'epoca che stiamo vivendo, vorrei chiudere ribadendo che l'IA

offre opportunità straordinarie, ma pone anche sfide enormi, in particolare per quanto riguarda la sicurezza nazionale nello spazio cibernetico, e non solo. In un simile scenario, caratterizzato dalla diffusione dell'IA quale potenziale strumento offensivo, difensivo e piattaforma di attacco, la resilienza si rivelerà un elemento ancor più cruciale per garantire la stabilità e la sicurezza del nostro Paese di fronte a minacce nuove, emergenti o semplicemente diverse.

Il futuro della sicurezza nazionale, ma anche quello della sicurezza di ciascuno di noi, dipenderà dalla nostra consapevolezza e capacità di integrare tecnologie avanzate, sviluppare strategie efficaci di difesa e resilienza, e garantire che le risposte agli attacchi siano coordinate e proporzionate alle minacce. In definitiva, la resilienza, abilitata dalla cultura, rappresenta non solo una strategia difensiva, ma anche una componente fondamentale della capacità di un Paese di prosperare in un ambiente sempre più digitalizzato e interconnesso.

LA PROCURA EUROPEA: UN NUOVO MODELLO DI PROCURA SOVRANAZIONALE INDIPENDENTE CHE GARANTISCE EFFICACIA E CONFORMITÀ GIURIDICA

Danilo Ceccarelli
EPPO - Senior Coordinator, Lotta alla criminalità organizzata

Introduzione all'EPPO

L'EPPO "è istituito come organo dell'Unione" (art. 3 del regolamento EPPO)[98], più precisamente come Procura dell'Unione. Ha il compito di "indagare, perseguire e giudicare" gli autori di reati che ledono gli interessi finanziari dell'Unione (art. 4) e agisce "nell'interesse dell'Unione nel suo insieme" (art. 6). All'interno dell'architettura istituzionale dell'UE, il ruolo dell'EPPO è molto particolare e senza precedenti. L'EPPO non si affida alle autorità giudiziarie nazionali. L'EPPO indaga e persegue direttamente negli Stati membri, senza intermediari nazionali, esercitando poteri di accusa e di indagine. In linea con l'articolo 86 del TFUE, l'EPPO esercita le sue funzioni davanti ai tribunali degli Stati membri.

Ciò si riflette in particolare nelle disposizioni (artt. 4, 13(1) e 28-40), che conferiscono ai procuratori delegati europei (PDE), che hanno sede negli Stati membri, almeno gli stessi poteri dei procuratori nazionali. Si crea così una struttura ibrida, in cui l'EPPO è l'ufficio del procuratore centralizzato dell'Unione, ma ha anche piena autorità giudiziaria all'interno del sistema nazionale di ciascuno Stato membro.

L'EPPO come procura pienamente indipendente

Una caratteristica specifica, e probabilmente la più importante, dell'EPPO è la sua indipendenza esterna. Negli Stati membri dell'UE esistono diversi modelli di azione penale. In alcuni Stati membri, il pubblico ministero ha forti legami con il potere esecutivo e può essere subordinato alle istruzioni del governo o deve riferire ad esso. In altri Stati membri, per bilanciare la mancanza di indipendenza del pubblico ministero, esiste un giudice istruttore (ovviamente indipendente) con forti poteri investigativi. In altri Stati membri,

98 Regolamento (UE) 2017/1939 del Consiglio, del 12 ottobre 2017, relativo all'attuazione di una cooperazione rafforzata sull'istituzione della Procura europea ("EPPO"), GU L 283 del 31.10.2017, 1. Nel presente documento, le disposizioni giuridiche citate sono tratte dal regolamento EPPO, salvo diversa indicazione.

invece, la procura è indipendente e i procuratori fanno parte a tutti gli effetti della magistratura. Il regolamento EPPO sottolinea la sua l'indipendenza, all'art. 6 e al considerando 16, vietando qualsiasi tipo di interferenza e influenza da parte di autorità dell'Unione e degli Stati membri e di persone esterne all'EPPO. All'art. 6 e nel considerando 16, vietando qualsiasi tipo di interferenza e influenza da parte di autorità dell'Unione e degli Stati membri e di persone esterne all'EPPO. Ai sensi degli artt. 6(2) e 7, l'EPPO è responsabile nei confronti dell'UE e degli Stati membri per le sue attività generali, ma non per le sue indagini e i suoi casi specifici, che sono protetti dalla riservatezza e soggetti solo al controllo giudiziario, in linea con l'art. 42 del regolamento e con il diritto nazionale.

Inoltre, l'EPPO non ha legami con il potere esecutivo nemmeno per quanto riguarda la sua politica generale in materia di procedimenti penali. Secondo l'art. 9 del Regolamento dell'EPPO, il Collegio dell'EPPO prende decisioni su questioni strategiche e ha il compito di garantire la coerenza, l'efficienza e l'uniformità della politica dell'azione penale dell'EPPO in tutti gli Stati membri. Concedere all'EPPO l'autorità di elaborare e decidere internamente la propria strategia e politica processuale, senza essere soggetto a istruzioni generali da parte del potere esecutivo, o a direttive, linee guida e istruzioni da parte di un'autorità processuale gerarchicamente superiore legata al governo, significa concedere all'EPPO piena indipendenza esterna e interna. Si tratta di un'ulteriore conferma dell'indipendenza dell'EPPO e di una chiara separazione dal potere esecutivo.

Infine, il considerando 16 del regolamento chiarisce il legame tra i poteri investigativi e processuali conferiti all'EPPO e la necessità di salvaguardarne l'indipendenza: "poiché all'EPPO devono essere conferiti poteri di indagine e di azione penale, è opportuno predisporre garanzie istituzionali per assicurarne l'indipendenza". Pertanto, le attuali norme statutarie e il quadro istituzionale garantiscono che l'EPPO, che agisce come ufficio unico in tutti gli Stati membri partecipanti, non sia esposto al rischio di essere soggetto a istruzioni o di essere obbligato a riferire all'esecutivo in casi specifici.

Tuttavia, la salvaguardia dell'indipendenza dell'istituzione potrebbe non essere sufficiente a proteggere l'indipendenza delle funzioni di pubblico ministero nel loro complesso. Come qualsiasi altra procura, l'EPPO svolge il suo mandato attraverso i suoi procuratori, ossia il procuratore capo europeo (PCE) e i procuratori europei (PE), che agiscono come membri delle Camere permanenti, nonché i procuratori delegati europei (PDE). Di conseguenza, dovrebbero essere predisposte garanzie istituzionali per proteggere l'EPPO in quanto ufficio unico, ma anche per tutelare l'indipendenza statutaria dei suoi procuratori e il loro *status* istituzionale. Le garanzie istituzionali per assicura-

re l'indipendenza dei procuratori comprendono la loro nomina, la progressione di carriera, l'inamovibilità, il licenziamento e l'azione disciplinare.

Per quanto riguarda la procedura di nomina, l'EPPO non può essere considerato pienamente indipendente, in quanto le autorità che nominano il procuratore capo europeo e il procuratore europeo sono istituzioni politiche dell'UE. Inoltre, la procedura di nomina dei procuratori europei è caratterizzata da una notevole mancanza di trasparenza. A seconda dello Stato membro interessato, anche le autorità politiche nazionali potrebbero avere un ruolo nella procedura di nomina - compresa quella dei procuratori delegati europei, dove in ogni caso la decisione finale è nelle mani del collegio dell'EPPO.

Inoltre, le autorità politiche possono ostacolare l'indipendenza della magistratura anche attraverso altri metodi più subdoli, come il taglio del budget operativo o la mancata assegnazione di risorse sufficienti alla procura, riducendone così costantemente l'efficienza e l'efficacia.

Il principio di legalità e il dovere di indagare e perseguire esclusivamente in conformità con la legge applicabile

In ogni caso, una volta nominati, i procuratori europei dell'EPPO godono delle necessarie garanzie istituzionali per proteggere la loro indipendenza.

Ciò è ancora più evidente se si considera che l'attività penale dell'EPPO - a differenza di quella di alcuni Stati membri partecipanti - è disciplinata dal principio di legalità, come sottolineato nei considerando 66 e 81 del suo regolamento. Ciò significa che l'EPPO non ha la facoltà di non indagare e perseguire un reato per il quale ha esercitato la propria competenza, come risulta anche dalla formulazione degli articoli 25(1), 35 e 36 del regolamento.

Come in ogni sistema democratico in cui il pubblico ministero gode di piena indipendenza, il potere esecutivo definisce le proprie decisioni politiche attraverso la legislazione. L'EPPO è soggetto, in primo luogo, al diritto dell'UE, a partire dalla Carta dei diritti fondamentali, e, in linea con il principio del primato del diritto dell'UE, alla legislazione nazionale, ove applicabile, a condizione che questa non sia in contrasto o incompatibile con il diritto dell'UE.

Di conseguenza, l'azione dell'EPPO è strettamente vincolata solo alla legge applicabile.

Ciò garantisce che la politica investigativa e processuale dell'EPPO sia giuridicamente prevedibile e in linea con la tutela dei valori sanciti principalmente dalla Carta dei diritti fondamentali dell'UE e dalle Costituzioni degli Stati membri dell'UE. Analogamente alla Corte di giustizia dell'Unione, l'EPPO difende i valori costituzionali dell'Unione europea, che sono condivisi dagli Stati membri e definiscono l'identità stessa dell'Unione europea

come ordinamento giuridico comune.[99] In questo contesto, l'EPPO è protetto dalle interferenze politiche nelle sue indagini, sia da parte delle autorità degli Stati membri che dell'Unione che - a seconda del contesto politico - potrebbero avere una lettura molto particolare del tipo di "interesse pubblico" che vogliono proteggere. In un ambiente sovranazionale e complesso come quello in cui opera l'EPPO, questa protezione è ancora più necessaria per avere un'azione investigativa e processuale guidata solo dalla legge e non da eventuali istruzioni di autorità politiche.

Questa necessità è ancora più evidente se riferita a fenomeni criminali come la cybercriminalità, che potrebbero minacciare le infrastrutture o le istituzioni democratiche e mettere in pericolo i valori fondamentali dell'Unione e dei suoi Stati membri. In queste situazioni, la legge dovrebbe essere l'unico elemento vincolante per l'autorità giudiziaria incaricata di attuare e confermare le contromisure e le risposte alla minaccia. Solo così si garantisce una protezione efficace.

Indipendenza, sovranazionalità ed efficacia dell'EPPO

In un contesto di criminalità transfrontaliera, ma anche senza frontiere, l'EPPO può essere presentato come un modello anche in termini di efficienza ed efficacia della sua azione.

La caratteristica più evidente dell'EPPO è la sua dimensione sovranazionale, essendo la prima procura in assoluto con poteri investigativi e processuali diretti in 24 Stati membri partecipanti.[100] In questo contesto, l'EPPO ha una conoscenza molto specifica delle questioni di giurisdizione transfrontaliera e un'esperienza unica dei sistemi operativi e giuridici degli Stati membri dell'UE, che l'EPPO sperimenta ogni giorno sul campo e nelle aule di giustizia nazionali.

L'EPPO è un ufficio unico, una dimensione che comprende sia la sua struttura centrale che quella decentrata e, in quanto tale, non soffre della frammentazione che, in diversi Stati membri, colpisce le procure, spesso organizzate in molti uffici separati - e talvolta in competizione tra loro -. uffici del

99 CGUE (Grande Camera), 16 febbraio 2022, causa C-156/21 (Ungheria contro Parlamento europeo e Consiglio dell'Unione europea), paragrafo 127.

100 La partecipazione degli Stati membri all'EPPO si basa sul principio della cooperazione rafforzata, in linea con gli articoli da 326 a 334 del Trattato sul funzionamento dell'Unione europea, che consente ad alcuni Stati membri di concordare il perseguimento di un obiettivo tra loro anche se gli altri Stati membri scelgono di astenersi dalla partecipazione. Il 1° giugno 2021, quando l'EPPO ha assunto le sue funzioni investigative e giudiziarie, 22 Stati membri erano membri dell'EPPO. La Polonia ha aderito all'EPPO il 29 febbraio 2024, mentre la Svezia ne è diventata membro il 16 luglio 2024. Ungheria, Irlanda e Danimarca non sono membri dell'EPPO.

pubblico ministero. L'EPPO svolge le sue indagini transfrontaliere non sulla base del principio di cooperazione o come rete di procuratori, ma come ufficio del procuratore in cui l'attività operativa è coordinata internamente. In questo modo, l'ufficio è in grado di raggiungere una coerenza molto diversa da quella sperimentata nella tradizionale cooperazione transfrontaliera in materia penale.

Tuttavia, l'EPPO opera allo stesso tempo in un sistema in cui le forze dell'ordine sono l'autorità nazionale. Pertanto, l'EPPO deve integrare l'attività delle forze dell'ordine nella sua struttura sovranazionale. Ciò avviene al di fuori degli strumenti tradizionali (UE e internazionali) di cooperazione reciproca, come l'Ordine Europeo di Indagine Penale (OEI) o la squadra, ma conferendo all'EPPO l'autorità di istruire e dirigere l'autorità nazionale durante lo svolgimento delle indagini, in linea con l'articolo 28 del regolamento, in tutti i suoi Stati membri. In questo modo, le forze dell'ordine nazionali che lavorano sotto la direzione dell'EPPO diventano in qualche modo "sovranazionali" nell'ambito delle indagini in questione.

Pertanto, l'efficienza e l'efficacia delle indagini transfrontaliere dell'EPPO sono, in larga misura, una conseguenza della natura sovranazionale e della struttura dell'EPPO. Naturalmente, per rendere tutto ciò possibile nella pratica, è necessario che l'EPPO disponga di sufficienti strumenti investigativi e analitici e di personale specializzato e qualificato che lavori a fianco delle forze dell'ordine nazionali, nella logica dell'"ufficio unico". Finora questo è stato garantito grazie all'Unità operativa dell'EPPO, ma un ruolo molto importante è svolto anche da EUROPOL che, pur non avendo l'autorità di "polizia giudiziaria" o "*law enforcement*", è l'Agenzia dell'UE che si trova nella posizione migliore per lavorare fianco a fianco con l'EPPO e le autorità nazionali, e ha un'eccezionale capacità di supporto analitico. Non c'è dubbio, infatti, che le organizzazioni sovranazionali dotate di autorità investigativa, operativa, processuale e - se necessario – giudiziaria, possano raggiungere un grado di efficacia nel perseguire la grave criminalità transfrontaliera altrimenti impossibile, seguendo il percorso tradizionale della cooperazione intergovernativa.

Questo è ancora più vero quando si combatte la criminalità informatica e la minaccia cibernetica, dove i confini e la giurisdizione sono labili e incerti. Indubbiamente, i fenomeni criminali in cui il concetto di giurisdizione territoriale è smaterializzato sono in crescita, e ciò rappresenta una sfida alle regole di giurisdizione tradizionalmente adottate dai sistemi giuridici, ma soprattutto alla capacità investigativa e operativa dei Paesi interessati. Le norme sulla giurisdizione in questo campo utilizzano sempre più spesso concetti come il "principio di protezione", che tiene conto dell'impatto della crimina-

lità informatica sugli interessi e sulla sicurezza dello Stato, o comunque del possibile effetto negativo causato nel Paese interessato. L'articolo 22 della bozza di convenzione delle Nazioni Unite contro la criminalità informatica [101]prevede che gli Stati parte abbiano la possibilità di stabilire la propria giurisdizione in base al principio della personalità passiva, ovvero se il reato danneggia lo Stato o i suoi cittadini. Dal punto di vista giuridico, queste norme potrebbero creare conflitti tra giurisdizioni concorrenti, ma non sono particolarmente problematiche.[102] Al contrario, lo scollamento tra i territori da cui il reato viene avviato e i territori interessati dalla condotta crea enormi difficoltà investigative e operative che è estremamente difficile superare attraverso i tradizionali strumenti intergovernativi di cooperazione reciproca, sia a livello di polizia che a livello giudiziario.

In questo contesto, l'EPPO potrebbe essere un ottimo esempio di autentica autorità sovranazionale, priva di vincoli giurisdizionali significativi nel suo "ambito giuridico" e dotata di un'ampia capacità investigativa e operativa sovranazionale nei suoi Stati membri, dove agisce in modo rapido ed efficace.

Conclusioni

L'EPPO esemplifica un modello unico di ufficio del pubblico ministero indipendente, che agisce sulla base del principio di legalità ed esclusivamente in conformità con la legge applicabile, in particolare seguendo il principio del primato del diritto dell'UE. Questo quadro giuridico sovranazionale si affianca a una capacità investigativa e a poteri giudiziari sovranazionali, dimostrando così una notevole efficacia operativa e garantendo la tutela dei valori democratici fondamentali.

---

101 "Progetto di convenzione delle Nazioni Unite contro la criminalità informatica - Rafforzamento della cooperazione internazionale per la lotta contro alcuni crimini commessi mediante sistemi di tecnologia dell'informazione e della comunicazione e per la condivisione di prove in forma elettronica di reati gravi", 7 agosto 2024.

102 In queste situazioni, l'articolo 22, paragrafo 6, del progetto di convenzione delle Nazioni Unite prevede solo "se opportuno" che le parti interessate "si consultino al fine di coordinare le loro azioni".

Amandeep Singh Gill

Inviato del Segretario Generale delle Nazioni Unite per la Tecnologia

Buongiorno, da New York.

Sono veramente lieto di poter condividere alcune osservazioni con voi e vorrei ringraziare la fondazione e la presidenza G7 italiana per questo onore. L'argomento che avete scelto per oggi è sicuramente importantissimo, in un momento in cui la tecnologia sta facendo grandi progressi in maniera talvolta imprevedibile. L'intelligenza artificiale, in particolare, è una di queste potenti tecnologie che sta rimodellando le nostre economie e presto rimodellerà le nostre società ed anche i nostri sistemi politici, fondamentalmente. Si tratta di una tecnologia che in qualche modo si comporta allo stesso modo dell'essere umano, negli stessi modi in cui gli uomini comunicano tra di loro. Con l'avvento dei modelli linguistici ampi vediamo come si agisce, come l'uomo agisce, così fa la tecnologia. Vi sono naturalmente delle implicazioni preoccupanti, ma allo stesso tempo delle opportunità entusiasmanti per poter compiere dei progressi per quanto riguarda gli obiettivi di sviluppo sostenibile e l'aumento della produttività nelle economie, ma anche nel contesto dell'invecchiamento della popolazione, perché potremmo anche avere delle soluzioni a più basso contenuto di manodopera.

A livello delle Nazioni Unite, stiamo cercando di capire qual è lo spazio per una governance internazionale di queste tecnologie. Infatti, molte azioni di governance e aspetti normativi saranno comunque gestiti da governi nazionali che prenderanno in considerazione anche le questioni di sicurezza nazionale, le situazioni culturali specifiche, fattori relativi alle specifiche società e allo stesso tempo anche fattori di concorrenzialità economica. Tuttavia, esistono delle azioni che in qualche modo appartengono al contesto internazionale. Tali azioni devono offrire un valore sia ai governi che al settore privato. Quindi, a livello delle Nazioni Unite, sappiamo perfettamente che dobbiamo basarci sui valori della Carta delle Nazioni Unite, della Dichiarazione Universale dei Diritti Umani, e sui trattati in materia di diritti umani. Fondamentalmente, dobbiamo basarci su valori fondamentali collegati ai diritti umani, alle libertà fondamentali, alla tutela della democrazia e dello stato di diritto.

Lo stesso tempo, considerata la sede delle Nazioni Unite, dobbiamo pensare anche a quali sono le implicazioni di queste tecnologie per la collaborazione internazionale. Ovvero, ci sono modi per ampliare la collaborazione internazionale utilizzando questa tecnologia, per in qualche modo diminuire la concorrenza che esisterà comunque, ma possiamo gestire la concorrenza in modo da creare uno spazio di collaborazione. Siamo stati quindi molto attivi negli ultimi due anni in questo senso e recentemente abbiamo avuto un

certo successo nei nostri vertici con l'adozione di un patto globale, ovvero il primo accordo universalmente accettato per la governance dell'intelligenza artificiale. Questo naturalmente si basa sui progressi fatti nel corso del processo di Hiroshima, portato avanti poi dalla presidenza italiana del G7, e ciò che è stato fatto a livello del Consiglio d'Europa e a livello dell'UNESCO.

Quindi, quali sono gli elementi principali di questo accordo universale sull'intelligenza artificiale che è stato preso nel settembre scorso? Noi dobbiamo, innanzitutto, osservare attentamente le capacità dell'intelligenza artificiale, quindi è necessaria una valutazione costante di queste capacità in modo da poter valutare indipendentemente la situazione, al di là di quello che dicono le aziende o i singoli paesi. Qual è il significato di questa tecnologia in termini di opportunità? E questo è un po' simile alla situazione del cambiamento climatico, dove noi abbiamo un gruppo intergovernativo che si occupa del cambiamento climatico. Però questa tecnologia si muove in fretta. Quindi dobbiamo agire in fretta e a livello pubblico, per offrire ai politici dei riferimenti su cui basare le proprie decisioni. Oltre a questo gruppo internazionale di scienziati, abbiamo i leader che, al vertice, hanno deciso che sarà necessario un dialogo politico costante. Questo è al cuore del problema che si discute nella conferenza attuale, ovvero come assicurare una certa interoperabilità tra le giurisdizioni, come garantire che le questioni relative alla criminalità, alla protezione delle libertà individuali e ai diritti fondamentali non vadano a scontrarsi. Ecco perché abbiamo diverse giurisdizioni e, come sappiamo, le Nazioni Unite sono una piattaforma inclusiva che consente a diverse giurisdizioni, che si tratti degli Stati Uniti, della Cina, dell'Unione Europea, di dialogare e condividere una serie di fattori per poter apprendere da questo scambio. Allo stesso tempo, si cerca di costruire un vocabolario comune per affrontare le problematiche utilizzando la base portante della Carta delle Nazioni Unite e altri strumenti giuridici preziosi.

Un terzo aspetto delle decisioni prese è quello di costruire capacità a livello mondiale, perché oggi il settore pubblico, in particolare le agenzie di polizia, sono un po' indietro per quanto riguarda la comprensione della tecnologia, visto che la conoscenza risiede principalmente nel settore privato. È importante riuscire a seguire queste tecnologie, agire in maniera saggia, e pensare anche all'equità, poiché esiste un digital divide. Ad esempio, tra i primi 50 paesi per quanto riguarda la capacità di intelligenza artificiale, non vi sono paesi africani; il primo paese africano è solo al 2000° posto nella lista delle capacità in materia di intelligenza artificiale. Ecco perché è fondamentale dare accesso anche ai paesi meno ricchi, preservando allo stesso tempo la differenza culturale e linguistica. Ad oggi, la maggior parte dei dati è presente in una sola lingua e fa riferimento a una zona geografica specifica, il che ha

implicazioni per il futuro. Sono questi tre settori in cui sono state prese delle decisioni, ma abbiamo ancora molto da fare. Naturalmente, il segretario generale delle Nazioni Unite ha deciso assolutamente di portare avanti questo tipo di lavoro, sostenendo sia il settore pubblico che quello privato, che ha anche delle responsabilità molto importanti, come sottolineato negli esiti degli incontri di Hiroshima.

L'intelligenza artificiale non è solo un argomento per esperti, ma è qualcosa che riguarda tutti, perché andrà a rimodellare le nostre società, il modo in cui avremo accesso alle informazioni, l'intermediazione in molti sensi, e anche gli impatti sui nostri rapporti tra persone. Tutti noi abbiamo una capacità mentale e un volere che vanno al di là delle capacità di qualsiasi chatbot. Questo naturalmente ha un significato, e implica discussioni sulla società. Ciò significa che i nostri sistemi normativi, i nostri meccanismi giurisdizionali, sono stati creati per lavorare in un mondo diverso. Questo implica che tutti noi dobbiamo riflettere su questi argomenti e agire. Ecco perché sono veramente contento che stiate prestando attenzione a questi temi. Lavoriamo in stretta collaborazione con la presidenza italiana del G7 per quanto riguarda gli impatti dell'intelligenza artificiale. Vi sono anche molti gruppi a livello internazionale, come il gruppo di Vienna, che trattano della criminalità, della cybercriminalità, dell'intelligenza artificiale e degli impatti come la disinformazione, e in che modo le minacce alla cybersicurezza dovranno essere affrontate nel futuro. Vi faccio i migliori auguri di buon lavoro e vi ringrazio ancora una volta. Desidero anche ricordare la persona alla quale è stata intitolata questa fondazione che ha organizzato l'evento.

DIBATTITO

Luigi Salvato:

Ringrazio il collega Danilo Ceccarelli che ha con tale passione e completezza verificato la possibilità di attraversare, di percorrere la strada di app per rafforzare la giurisdizione in materia di Cyber Crime. Sintetizzare la sua relazione in una domanda un po' ingenua e un po' provocatoria: ma allora pensiamo di estendere la competenza di EPPO anche ai reati in materia di Cybercrime? Comunque, lasciando da parte questa domanda, abbiamo concluso. C'è qualcuno? Ci sono altre domande?

Eric Do Val Lacerda Sogocio:

Grazie delle presentazioni. Io ho una domanda abbastanza semplice per due dei relatori.

Per il prof. Roscini: ho sentito la sua presentazione, ha parlato di contromisure e di due diligence, ma la mia piccola domanda è: non sarebbe preoccupato di una situazione in cui i procuratori potrebbero commettere dei reati in giurisdizione? Potrebbero commettere il reato di accesso illegale o abuso di un dispositivo, un cattivo uso di un dispositivo, nel perseguire delle contromisure, così come lei ha spiegato? Ma la stessa domanda vorrei farla al dottor Ceccarelli: come non sarebbe preoccupato di commettere un reato, in un'altra giurisdizione, nell'investigazione?

Marco Roscini:

Non è una domanda semplice. Sarei preoccupato, però credo che dobbiamo scegliere tra fare qualcosa che potrebbe esse illegale secondo il diritto penale internazionale e non fare niente. Questa è la scelta. Non si può arrivare così a una strada senza uscita perché c'è l'elemento della condotta, magari lecita, che si fa sotto lo scudo della sovranità. Ma alla fine, se è possibile, c'è da fare questa scelta, ma bisogna bilanciare i diversi interessi: l'interesse dello stato il cui territorio è stato violato e il diritto dell'altro stato. Insomma, ci sono certo dei casi in cui si è cercato di bilanciare i diversi interessi. Ho fatto riferimento a quel caso norvegese.

La parola "sovranità" forse è quella più ripetuta in questa conferenza, ripetuta in questi due giorni, e viene usata spesso come un valore buono di per sé. Ma il diritto internazionale non tutela la sovranità per sé, bensì protegge quella che rispetta la legge. Quando una sovranità viola l'altra sovranità, tante tutele scompaiono e quindi arriviamo alle contromisure.

Questo è il principio di non intervento, che tutela uno Stato soltanto quando agisce, anche internamente, secondo le regole. Quindi la mia risposta non è una risposta: posso dire solo che dobbiamo bilanciare i diversi interessi. Lo Stato vuole che la sua sovranità sia protetta, ma c'è proprio questo divario tra la giurisdizione prescrittiva e quella attuativa di cui avevo parlato prima.

Danilo Ceccarelli:

Sono d'accordo con la risposta del professor Roscini e sono d'accordo anche con la maggior parte delle cose che ha detto nella sua presentazione. Però le voglio dire qualcosa: i procuratori e gli enti di polizia commettono dei reati tutti i giorni. Intercettiamo delle persone, arrestiamo delle persone privandole della libertà, congeliamo e sequestriamo dei beni, e lo facciamo tutti i giorni. Mettiamo le persone in prigione, a volte anche per molto tempo, cosa che fanno magari più i giudici. Ma questo può essere un reato di per sé, cioè lo Stato si difende, difende la propria comunità contro le attività illegali. La grande differenza è che questo si fa secondo la legge, e ogni volta che facciamo un passo accettiamo un rischio. Sì, è vero, può essere vero che noi non rispettiamo la legge e commettiamo un reato violandola. Forse non rispettiamo, ed è una cosa di cui ha parlato il professor Roscini, il principio di proporzionalità.

Pensiamo a quello che sta succedendo nel mondo oggi. Ma dobbiamo reagire secondo la legge, in buona fede, nel miglior modo possibile contro l'illegalità, perché se non lo facciamo, la società... eh, non so come farebbe a funzionare senza legalità.

Quindi è un rischio che accettiamo, fa parte del nostro lavoro, e questo include situazioni in cui bisogna prendere un'iniziativa e agire contro qualcuno che si trova in un paese terzo o anche contro un paese terzo, sempre rispettando la legge e il principio di proporzionalità.

CONCLUSIONI

Alfredo Mantovano
Sottosegretario di Stato alla Presidenza del Consiglio dei Ministri

Chiedo scusa per non essere in mezzo a voi come avrei desiderato, saluto tutti voi e ringrazio la Fondazione Occorsio per l'invito e un saluto tutto particolare al presidente Giovanni Salvi. Con questo seminario voi avete fatto una cosa importante, avete richiamato la necessità di un'approfondita riflessione sulle garanzie di giurisdizione nella resilienza e nella difesa della sicurezza nazionale dello spazio virtuale. Il progressivo sviluppo delle tecnologie digitali, dall'intelligenza artificiale alle cripto valute, pone, come sappiamo, gli Stati e, al loro interno, le giurisdizioni, di fronte a sfide e a minacce innovative che sfruttano spazi dalle caratteristiche del tutto inedite in senso tradizionale; la categoria della extra territorialità, correlata a spazi fisici sui quali gli Stati non hanno la giurisdizione, salvo qualche fantasia interpretativa, che in questo momento non ci interessa. Parlando di Cyber invece l'extra territorialità fa riferimento a spazi che sono privi di qualsiasi connotazione geografica e che tecnicamente sono illimitati nella dimensione. Sarebbe meglio dire che si tratta di fenomeni a-territoriali come suggerito da alcuni autori, per evidenziare che la loro caratteristica strutturale è proprio la mancanza di un territorio fisico. Opportunamente il seminario ha identificato in questa cornice una serie di problemi nuovi e complessi sui quali riflettere, come per esempio individuare un efficace criterio di collegamento territoriale che radichi la giurisdizione degli Stati in relazione a quanto avviene nella realtà virtuale. Ciò vale anzitutto sul piano della repressione dei crimini, ma non soltanto: penso ai profili di rilevanza economica, per esempio quale impatto ha l'intelligenza artificiale sui diritti fondamentali e sull'organizzazione delle funzioni pubbliche, compresa la giurisdizione. Per esempio, con quali modalità si può tutelare in modo efficace la resilienza delle infrastrutture critiche digitali e quali sono i problemi legati alla individuazione della reale regia degli attacchi cyber, ossia il tema complesso, sia dal punto di vista tecnico-informatico, che politico o diplomatico, della cosiddetta *attribution;* con quali modalità infine coordinare a livello internazionale strategie di contrasto al crimine transnazionale del mondo digitale.

Il governo non si tira indietro, per la parte di sua competenza, nel fornire una risposta efficace a queste sfide. Ricordo, tra l'altro, le novità apportate dalla Legge n. 90 del 28 giugno di quest'anno per garantire il rafforzamento

della cybersecurity nazionale, che certamente tutti avete letto, approfondito e di cui avrete discusso; penso ancora all'adozione del D.lgs. 4 settembre 2024 di recepimento della direttiva NIS2 e al disegno di legge in materia di IA, attualmente in discussione in Senato, che punta a coniugare le potenzialità della IA con il rispetto dei diritti fondamentali e identifica le linee guida per il suo utilizzo nell'ambito delle funzioni pubbliche, incluso l'ambito giudiziario.

La cooperazione internazionale gioca un ruolo fondamentale e per questo oltre agli sforzi profusi sul piano europeo stiamo cogliendo l'opportunità dellaPresidenza del G7: come presidenza italiana abbiamo istituito un nuovo gruppo di lavoro specificamente dedicato alla cybersecurity, al cui interno confrontarci con i nostri partner in ordine all'affinamento degli strumenti di contrasto ai principali fenomeni cyber che minacciano la nostra sicurezza, *in primis* gli attacchi *ransomware*. C'è ancora tanto da fare e in tal senso iniziative come quella da voi organizzata sono certamente utili e preziose e vi ringrazio.

SINTESI DEI LAVORI

Giovanni Salvi

Io in realtà non solo non farò delle conclusioni, ma non farò nemmeno una sintesi dei lavori, perché ci vorrebbe un'altra mezza giornata per la complessità delle questioni che sono state affrontate. Dirò solo, a modo di sintesi conclusiva, che il gruppo di lavoro che ha elaborato questo programma forse non ha sbagliato nello strutturare la progressione, perché alla fine siamo arrivati, nell'ultima giornata, al nodo del nostro tema, come è reso evidente anche dallo scambio di battute divertente tra Sogocio e i nostri relatori di oggi. Divertente perché va a un punto vero, un punto che non è superabile, almeno per me, in questo momento. Io non vedo una soluzione. La proposta che è venuta fuori nel nostro lavoro preparatorio, e che vedo oggi ha trovato elementi di conferma, è che occorre distinguere nettamente, anche per ciò che concerne le attività della giurisdizione in uno spazio virtuale nel cyberspazio, tra ciò che è l'ordinaria attività giudiziaria, per la quale possono valere gli strumenti di cooperazione attuali, anche quelli più moderni che siamo immaginando, quelli previsti dal regolamento dell'Unione Europea sulle evidenze virtuali (e-evidence) e quelli previsti dalla convenzione di Budapest e dalla futura convenzione sul cybercrime.

Queste sono forme di cooperazione efficaci e saranno sempre più efficaci. Ma c'è un punto che invece non può essere affrontato così, proprio per le caratteristiche specifiche di questo settore, perché vi sono attività criminali, o comunque attività che richiedono accertamento, che non possono essere accertate successivamente, nemmeno nel breve spazio di ore necessarie per richiedere la cooperazione da parte di un'altra autorità giudiziaria. Questo, a mio parere, è un dato da cui bisogna partire.

Solo seguendo immediatamente la traccia, e non sempre ciò sarà sufficiente, si potrà ottenere la raccolta e il consolidamento di alcuni elementi di prova, a volte essenziali. Lo stesso problema si pone per la giurisdizione penale e per il diritto pubblico internazionale sotto il profilo dell'attribuzione. È esattamente lo stesso problema. Evidentemente è diversa la qualità della prova, così come è diverso il ragionamento che porta alla conclusione. Ma il problema è lo stesso.

Qui quella questione resta. Resta perché, entro certi limiti, la proposta che veniva fuori da tanti interventi è quella di utilizzare ciò che è previsto sia dalla convenzione di Budapest sia dalla futura convenzione sul cybercrime: il

passaggio dagli *Investigative Teams* agli *Investigative Bodies*, cioè strutture stabili che prescindono dalla commissione del reato e stabilizzano il consenso prima che il reato sia commesso.

Queste consentono attività immediate anche da parte dello Stato attaccato, salvo i meccanismi di convalida, in qualunque momento l'attacco avvenga e da dovunque l'attacco provenga. Questo è difficile, ma è una strada percorribile. Non è la strada della procura europea, perché quella è la strada dell'esercizio della giurisdizione dall'inizio alla fine su reati attribuiti.

Io credo che sia molto presto per prevederlo, ma possiamo utilizzare l'esperienza della Procura Europea e, soprattutto, i meccanismi utilizzati per assicurare l'indipendenza di un organo dipendente dall'Unione, per immaginare la costruzione di una fiducia tra gli stati che intendessero partecipare a questa forma di condivisione delle strutture.

Ci sono già strutture di polizia che possono essere meglio organizzate intorno a questi obiettivi. Ma una volta fatto questo, e avendo cento Stati nazionali che partecipano agli *Investigative Bodies* che consentono la cessione di una piccola parte di sovranità, non quella giurisdizionale sull'intera procedura, ma quella necessaria per acquisire immediatamente informazioni che altrimenti si perderebbero. Però rimangono altri novanta Stati.

La questione di cui avete discusso in maniera così efficace, soprattutto da parte di Sogosio, del professor Roscini e nella risposta di Ceccarelli, rimane. Resta soprattutto nei confronti degli Stati più pericolosi e degli attacchi più pericolosi.

Lavorare su questo è il nostro obiettivo. Per la Fondazione Occorsio, il lavoro di oggi ha due funzioni: portare le conoscenze acquisite nella pratica quotidiana e unirle alla formazione per magistrati e forze di polizia. Ringraziamo tutti i relatori e soprattutto i giovani che hanno collaborato, mostrando il meglio dell'Italia, nonostante le difficoltà e i sacrifici.

Infine, un pensiero affettuoso a Eugenio Occorsio, che in questo momento sta affrontando una sua battaglia personale. La sua figura, e quella del padre, ci ricordano l'importanza del nostro impegno per la legalità.

***

Michele Giacomelli

È stato un piacere avervi qui alla Farnesina. È stato molto istruttivo, molto interessante ed è per noi un motivo di vanto aver dato una mano alla Fondazione Vittorio Occorsio per organizzare questa iniziativa, collaborare con voi e contribuire all'arricchimento scientifico e umano della nostra attività. Grazie mille a tutti.