ATTUAZIONE DELLA GIURISDIZIONE PENALE NELLO SPAZIO VIRTUALE E SICUREZZA NAZIONALE

Intervento di apertura dell'anno accademico della Scuola Superiore di Polizia 2022/2023
Roma, 27 ottobre 2022

di Giovanni Salvi

La guerra in Ucraina ha reso evidente l'importanza dell'impiego di tecniche avanzate, tra cui diverse forme di intelligenza artificiale.

Droni in parte autonomi hanno avuto una funzione essenziale nel contrastare i movimenti di armate tradizionali e nell'individuare e distruggere centri di comunicazione e comando. Le immagini che vediamo quotidianamente prefigurano una guerra tra macchine e fanno immaginare sviluppi nell'autonomia decisionale del drone che pongono seri problemi etici.

Temi in realtà non dissimili da quelli che già oggi si affrontano nell'uso quotidiano dell'intelligenza artificiale, ad esempio per le auto a guida autonoma. Essi hanno reso di palmare evidenza il dilemma del carrello ferroviario, delle scelte tragiche, già celebre da anni tra gli studiosi di filosofia morale e sul quale hanno scritto pagine memorabili studiosi quali Hannah Arendt e Guido Calabresi. Scelte che ora vengono traslate nell'algoritmo di auto apprendimento.

Il conflitto ha poi reso evidente l'importanza della comunicazione pubblica, anch'essa condizionata dall'uso della intelligenza artificiale.

La lotta per le coscienze non nasce certo con l'intelligenza artificiale e neppure nascono con essa le tecniche di disinformazione. Basti pensare, per la disinformazione attraverso la diffusione di informazioni, ai Protocolli dei Savi di Sion, oppure, per la manipolazione delle immagini, alla cancellazione dei personaggi vittime di purghe, di sovietica memoria ma praticata da ogni regime totalitario che punti alla creazione e al controllo di un'opinione pubblica ad essa coerente.

La guerra ha però reso evidente la profonda trasformazione che entrambe queste tipologie di disinformazione subiscono, quando effettuate attraverso l'impiego di tecnologie di intelligenza artificiale.

Si sperimentano nel conflitto le tecniche già impiegate nel tentativo di condizionare le elezioni in alcuni paesi, come gli Stati Uniti nel 2016, la Gran Bretagna in occasione della Brexit, la Francia nelle elezioni presidenziali.

Editore Associazione "Progetto giustizia penale" | via Festa del Perdono 7, 20122 Milano
c/o Università degli Studi di Milano, Dipartimento di Scienze Giuridiche "Cesare Beccaria"
redazione@sistemapenale.it

La comprensione della gravità della sfida verso un valore fondante della democrazia rappresentativa, la fiducia, hanno portato alcuni Paesi ad assumere iniziative volte anche alla previsione di fattispecie di reato. L'Unione Europea a sua volta ha affrontato il tema dal punto di vista della prevenzione. In Italia già da alcuni anni sono state presentate delle iniziative parlamentari, non andate a buon fine.

La questione della disinformazione è ormai al centro delle preoccupazioni delle nostre strutture volte a proteggere il paese nel perimetro della sicurezza cibernetica.

Ciò che può essere tutelato attraverso le sanzioni (e tra queste inserisco anche quelle di carattere non penale, come la chiusura di siti o di piattaforme o l'interruzione della propagazione di contenuti) non è la "verità", cioè il contenuto della informazione. Vi sono limiti alla possibilità di attribuire allo Stato la decisione su ciò che costituisce verità, per il rischio che ciò incida su basilari principi costituzionali e valoriali dello Stato di diritto, tra cui la libertà di manifestazione del pensiero. Sia chiaro, in molti casi l'accertamento della corrispondenza a verità fattuale del contenuto di una affermazione non è in contrasto con tali principi. Tale accertamento è quotidianamente operato nelle aule di giustizia, ad esempio in tema di verità dell'addebito nella diffamazione o – per restare ad un caso prossimo a quello della manipolazione politica – in materia di *market abuse*.

Può essere tuttavia tutelata senza particolari problemi di compatibilità costituzionale la correttezza nella comunicazione. Dobbiamo cioè sapere, nello spazio destinato al dibattito pubblico, se un video è stato generato da un sistema di intelligenza artificiale o se esso è invece la rappresentazione di un evento reale. Alla stessa maniera dobbiamo sapere se esso è stato trasmesso da un BOT, cioè da una macchina autonoma, o da esseri umani nello svolgimento diretto di una attività consapevole. Dobbiamo poi essere in grado di conoscere la provenienza della informazione, attraverso la previsione della possibilità di risalire a ritroso la catena della informazione, fino ad arrivare all'entità che l'ha prodotta o diffusa.

Rispetto alle tecniche di disinformazione del passato, le attuali si differenziano per caratteristiche che – considerate unitariamente – ne trasformano ontologicamente la struttura.

Non si tratta solo del numero impressionante di ri-trasmissioni che un BOT è in grado di fare, rispetto a un essere umano o gruppo di esseri umani, ma delle loro intrinseche caratteristiche anche relative al contenuto, per la capacità della macchina di apprendere e di reagire.

Vi sono molte definizioni di Intelligenza Artificiale (IA). Alcune di queste sono normative, più che descrittive; esse rispondono all'esigenza di dare una definizione di ciò che vorremmo, dal punto di vista della normazione, che l'IA fosse, piuttosto di ciò che è o può essere.

Ad esempio, il Parlamento Europeo, nella risoluzione del 2021 su *Intelligenza artificiale: questioni relative all'interpretazione e applicazione del diritto internazionale (al di*

fuori degli aspetti penali) fornisce la seguente definizione, nella quale abbiamo evidenziato concetti che non sono affatto pacifici o connaturati alla IA:

> "sistema di intelligenza artificiale (IA)": un sistema basato su software o integrato in dispositivi hardware che mostra un comportamento che simula l'intelligenza, tra l'altro raccogliendo e trattando dati, analizzando e interpretando il proprio ambiente e intraprendendo azioni, con un certo grado di autonomia, per raggiungere obiettivi specifici.

Che l'IA *simuli* quella umana è un nostro desiderio, forse pregiudizio. In realtà, lo sviluppo impetuoso delle capacità di calcolo e di comunicazione (e di interconnessione), fa sì che la capacità della macchina di imparare (*Machine Learning*) dalle infinite fonti e connessioni porti verso lidi inesplorati; lo stesso può dirsi per la specificità degli obiettivi della macchina. Tra breve ne discuteremo, quando parleremo di come l'IA si sposti dal perseguimento di obiettivi specifici a temi generalisti.

Che poi l'IA operi con "un certo grado di autonomia" è anch'esso un nostro auspicio, perché la limitazione di grado rende possibile l'opposto, cioè il controllo da parte dell'agente umano, ma tale grado dipende da una serie di fattori e di limiti, anche esterni, che non costituiscono componente necessaria della IA.

Queste caratteristiche non riguardano solo la disinformazione, oggi in evidenza e da cui siamo partiti, ma molte forme di interferenza nella vita sociale, a fini illeciti o - come si dice nel gergo- malevoli (*malicious*).

Può trattarsi della manipolazione del mercato a fini di profitto o di attività a fini di terrorismo, dal proselitismo al diretto attacco di infrastrutture. Può trattarsi, più comunemente, del riciclaggio attraverso valori virtuali (tra cui le cosiddette *virtual coins*) o la pedopornografia o le estorsioni consumate attraverso la generazione di immagini virtuali assolutamente realistiche.

Una schematizzazione aiuta a comprendere, ad esempio, il danno che deriva dall'utilizzo di manipolazioni (disinformazione, deep fake ecc.). Evidenzio in rosso quelle che ritengo di maggiore rilevanza e novità.

Psychological harm	Financial harm	Societal harm
• (S)extortion • Defamation • Intimidation • Bullying • Undermining trust	• Extortion • Identity theft • Fraud • Stock-price manipulation • Brand damage • Reputational damage	• News media manipulation • Damage to economic stability • Damage to the justice system • Damage to the scientific system • Erosion of trust • Damage to democracy • Manipulation of elections • Damage to international relations • Damage to national security

Molte di queste applicazioni delle nuove tecnologie sono già punibili, perché previste da vecchie o nuove previsioni, o perché le vecchie fattispecie si applicano senza particolari problemi alle nuove condotte, o infine perché il legislatore ha introdotto nuove ipotesi, in grado di dialogare con gli aspetti innovativi delle tecnologie avanzate. Tuttavia, i problemi non sono risolti per il solo fatto che alcune delle condotte sono già perseguibili.

Abbiamo una notevole esperienza, come magistratura e forze di polizia, delle difficoltà di accertamento di questi reati, quando commessi con capacità professionalmente elevate, magari in forma organizzata. È questa la nuova sfida del *cyber crime*. Reati per i quali l'impiego di questa tecnologia non è solo una nuova opportunità ma costituisce una profonda trasformazione nella struttura del reato e anche in quello della responsabilità dell'agente.

Il tema della responsabilità individuale si porrà con sempre maggiore forza, mano a mano che l'intervento dell'intelligenza artificiale nel processo decisionale della macchina diverrà più significativo. Si pensi alla complessità del tema della responsabilità nell'utilizzo delle autovetture a guida autonoma. La distribuzione della responsabilità tra le diverse componenti che concorrono all'esito finale si modifica radicalmente a seconda delle caratteristiche tecniche dello strumento e in particolare dell'algoritmo che lo governa. Una macchina in cui la guida autonoma si limita all'assistenza al parcheggio, alla frenata di emergenza, alla segnalazione dell'ostacolo o del salto di corsia non altera significativamente la responsabilità del conducente e neppure il rapporto tra questa responsabilità e quella del produttore o del manutentore della macchina o della strada percorsa. Ben diverso è il tema quando, come già avviene e come sarà ancora più evidente in futuro, il conducente verrà progressivamente

estromesso dalla effettiva decisione sulla guida della macchina, mentre nella conduzione concorreranno la strada interattiva e l'algoritmo di guida del mezzo.

Nell'attuale condizione, sia della tecnologia applicata sia dell'elaborazione giuridica sul tema, il conducente non può dismettere la responsabilità della guida e ha comunque un obbligo di sorveglianza e di attivazione. Già ora, tuttavia, la capacità della macchina di reagire a situazioni impreviste e in genere di mantenere il mezzo in condizioni di corretta gestione, è superiore rispetto a quella del miglior conducente umano.

Questa differenza aumenterà nel tempo via via che l'apprendimento automatico della macchina, il *machine learning*, renderà la macchina ancora più efficace. Questo, tuttavia, non eliminerà del tutto la possibilità dell'incidente, per malfunzionamento o per situazioni che possono dalla macchina essere male interpretate, o infine per scelte etiche che la macchina potrebbe elaborare in maniera difforme dalle previsioni originarie, impostate dal creatore dell'algoritmo.

Naturalmente sono previsti meccanismi, già nella fase di costruzione dell'algoritmo e soprattutto della interconnessione tra la macchina e il contesto comunicativo nel quale la macchina dovrà operare, che riducono drasticamente anche questi rischi.

Ad esempio, mentre il conducente umano è isolato e riceve solo degli input esterni non tra loro correlati, come l'immagine che percepisce attraverso la vista, il suono, l'elaborazione della visione della segnaletica stradale, la macchina è direttamente connessa alla strada interattiva e di conseguenza alla segnaletica e in un prossimo futuro anche con tutti gli altri mezzi che circolano nello stesso contesto, così anticipando di molto qualunque processo decisionale necessario.

E pur tuttavia residua un'area di imponderabilità rispetto alla quale il tema della responsabilità diviene davvero complicato, anche a causa della interazione tra sistemi diversi e soprattutto, a mio parere, per la imprevedibilità da parte del creatore dell'algoritmo degli sviluppi che il *machine learning* avanzato, in ambiente interconnesso, può determinare nell'esito finale della reazione della macchina; tanto più che questa può utilizzare, nella interpretazione del dato e poi nella reazione, una logica non causale. È in questo senso che si parla più approfonditamente di responsabilità della macchina, quale distinta dal singolo operatore umano.

È un tema affascinante che si lega certamente a quello della società del rischio ed è pertanto non particolarmente nuovo, così da portare verso forme di responsabilità analoghe a quelle previste nel nostro ordinamento dalla legge 231 del 2001 in tema di responsabilità degli enti, ma che in termini di di lunga prospettiva, quasi filosofici, va oltre e fa prefigurare un autonomo processo decisionale svincolato dall'algoritmo originario.

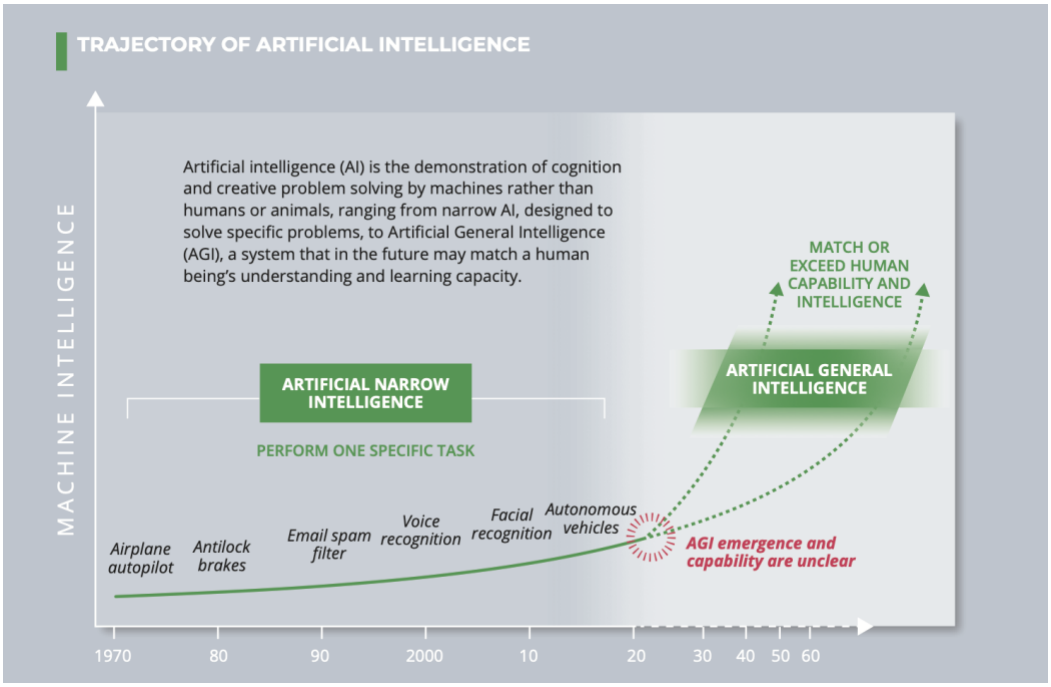
Una creatura che si ribella al suo creatore. Angelo caduto che raccoglie la mela della conoscenza che le è negata dall'algoritmo creatore.

Questa visione non è in realtà fantascienza, peraltro già immaginata negli anni '50 da Isaac Asimov, scrittore di grandi romanzi e anche scienziato, che previde le Tre Leggi della Robotica, non dissimili dai princìpi etici che governano oggi l'intelligenza artificiale a scopi pacifici, ma che sono in realtà travolti dall'uso militare o offensivo della robotica.

Sullo sfondo vi è il passaggio dall'intelligenza artificiale applicata -cioè limitata alla gestione di singole attività specifiche, anche di estrema complessità ma comunque ben delimitate dalla macchina e dall'algoritmo che la fa agire, detta IA ristretta - da forme di intelligenza artificiale generale. L' enorme capacità di calcolo dei nuovi computers e le caratteristiche di funzionamento di computers basati sulla logica quantica, il *quantum computing*, consentono di prevedere che l'intelligenza artificiale possa svilupparsi verso forme di conoscenza difficilmente distinguibili dalla coscienza, dalla percezione di sentimenti ed emozioni.

È però una banalizzazione affermare che tale intelligenza simuli quella umana. Non sappiamo se ciò sia vero, se questa sia solo una metafora o se in realtà questa forma di intelligenza si indirizzi verso luoghi a noi del tutto sconosciuti. Lo sviluppo dell'intelligenza artificiale generalista è individuato tra le principali sfide esistenziali raccolte nel *GlobalTrends* per il 2040 del *National Intelligence Council* statunitense.

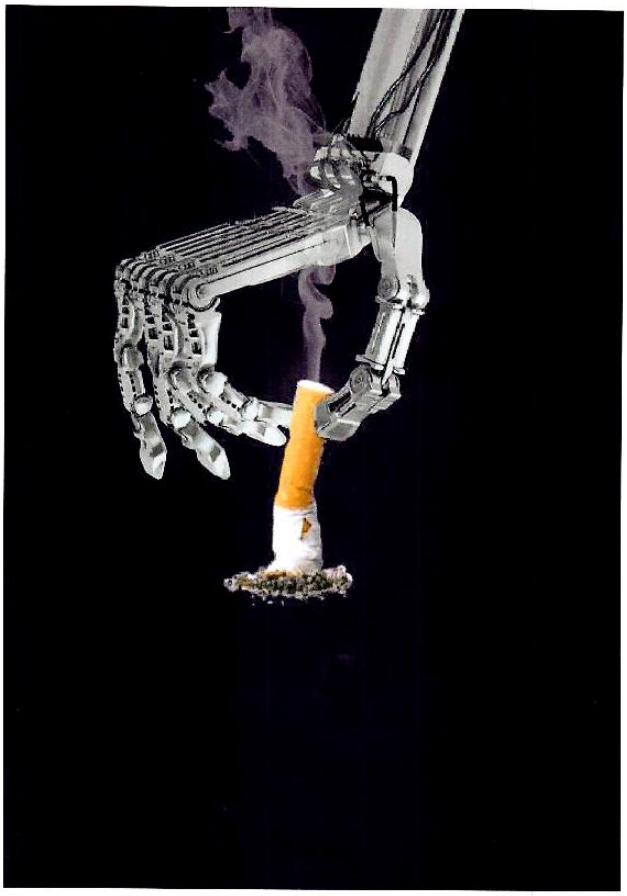
In un diagramma di questo lavoro che ha per scopo di indirizzare le attività delle agenzie statunitensi, si individua con chiarezza la progressione della tecnologia dell'intelligenza artificiale.



E proprio negli anni in cui siamo che la linea si impenna verso l'IA generale. Ciò è dovuto anche all'avvento del *Quantum Computing* che, oltre a sviluppare enormi potenzialità di calcolo, annulla i tempi di latenza e opera secondo logiche non causali, diverse da quelle del nostro ragionamento induttivo-deduttivo.

In un altro analogo lavoro, volto a illustrare gli sviluppi dell'intelligenza artificiale verso attività generaliste, è rappresentata una mano meccanica che spegne una candela. A mio parere l'immagine non coglie fino in fondo le sfumature essenziali, o meglio non le fa comprendere ad un uomo vissuto alla fine del ventesimo secolo. Spegnere una candela è una attività meccanica, non particolarmente coinvolgente. Forse lo sarebbe stato nel diciannovesimo secolo, quando la candela era parte della vita quotidiana. Ho fatto una piccola modifica, certo non utilizzando il GAN (*Generative Adversial Network*) e il risultato lo dimostra.

Spegnere una sigaretta, almeno per un uomo della mia età, ha invece un profondo significato emozionale. La macchina è stanca e si è presa una pausa prima di tornare al lavoro; oppure ha avuto un'esperienza piacevole e ha fumato tranquillamente la sua sigaretta:



Questa immagine a mio parere rappresenta meglio, anche se non compiutamente, quello che potrebbe essere lo sviluppo prossimo di un'intelligenza artificiale generale.

Naturalmente questi aspetti non sono solo negativi. Al contrario, lo sviluppo di queste tecnologie informatiche avanzate costituisce una enorme opportunità per migliorare la nostra vita quotidiana, in direzione che pochi anni fa sarebbero state impensabili, dalla sicurezza dei trasporti fino alla telemedicina che già adesso consente un generalizzato uso, anche a fini imprenditoriali, di tecniche informatiche.

Anche le monete virtuali, a cui abbiamo fatto cenno all'inizio del nostro intervento indicandole come un potenziale strumento che facilita le attività illecite, costituiscono in realtà uno straordinario strumento di libertà nelle transazioni e, paradossalmente, di loro tracciabilità.

Le monete virtuali costituiscono il caso più conosciuto di una realtà più complessa, rispetto alla quale sarebbe ormai meglio parlare di asset virtuali, di risorse virtuali. È ormai possibile attribuire a qualunque entità un valore scambiabile nel mercato virtuale. Può trattarsi di entità con una loro oggettività dura, materiale, o di entità immateriali cui si attribuisce un valore scambiabile. Il Bitcoin, origine delle molte

monete virtuali oggi correnti, si basa sull'idea della catena non modificabile di blocchi di informazioni. La *blockchain*, dunque, in realtà costituisce una traccia non modificabile e non eliminabile dell'intero percorso della transazione, dall'origine della moneta virtuale fino al detentore attuale. Nata come strumento di disintermediazione e di anonimizzazione parziale, essa diviene progressivamente uno strumento monetario regolamentato. La semi-anonimità rende accessibile anche l'informazione sul soggetto, almeno in alcune fasi del passaggio dalla moneta Fiat (cioè operante nel mercato reale) a quella virtuale, o in quella in cui la moneta è gestita da operatori. Tuttavia, la richiesta maggiore dell'utente della moneta virtuale, quando non ha finalità speculative vista la grande volatilità di quel mercato, è proprio di restare anonimo. Vi sono molti modi con cui questa esigenza può essere realizzata, da programmi che aiutano a rendere impossibile seguire la traccia individuale, fino alla totale realizzazione delle transazioni nel mercato virtuale e in ambienti dedicati, il dark web, così da evitare la pericolosa fase dell'ingresso e dell'uscita dall'ambiente virtuale.

Per chi fosse interessato a conoscere più specificamente questi temi, rinvio al laboratorio utilizzato nel corso Vittorio Occorsio, organizzato dalla omonima Fondazione e tenuto presso la Scuola di Perfezionamento delle Forze di Polizia, di imminente pubblicazione sulla rivista di quella Scuola. Mi riferisco naturalmente ai non specialisti, visto che siamo in un luogo – la Scuola superiore della Polizia di Stato – nel quale queste conoscenze sono molto diffuse, anche perché la Polizia delle Comunicazioni è il massimo organo deputato al contrasto delle attività illecite sul web.

Dunque, ogni applicazione della IA può avere più facce. Pensate, sempre rimanendo al nostro campo, alle molte applicazioni utili per agevolare il lavoro degli operatori giudiziari e della stessa polizia giudiziaria. Nel primo ambito, sono ormai di uso comune in molti Paesi e lo sta divenendo anche nel nostro, l'utilizzo della IA per "prevedere" l'esito di un giudizio. Queste applicazioni non sostituiscono il giudice o le parti, ma danno loro uno strumento utile per valutare le possibilità di vittoria, nel civile, e dunque anche l'opportunità di instaurare la controversia. Molto sperimentata è l'utilizzazione della IA c.d. predittiva per diagnosticare le probabilità di recidiva o, nelle applicazioni strettamente preventive, di commissione di alcune tipologie di reati, anche in relazione ad aree territoriali. E' lo scenario anticipato già negli anni '50 dal grande scrittore Philip Dick in *Minority Report*, dove veggenti anticipano alla fase strettamente ideativa la scoperta del crimine e dunque anche la sua punizione.

Queste applicazioni soffrono del c.d. *Bias*, cioè dell'effetto del pre-giudizio sulla predizione. E' anche per questa ragione che la giurisprudenza ha elaborato strumenti di cautela, tra cui innanzitutto la necessità che siano conosciuti dalla controparte i meccanismi di funzionamento dell'analisi e della elaborazione (i c.d. Algoritmi).

Noi oggi ci concentriamo sulle conseguenze malevole, dannose, dell'impiego della IA, sia nella vita quotidiana, sia specificamente a fini criminali.

Esse sono contrastate innanzitutto in via preventiva, attraverso la progressiva regolamentazione che si sta scrivendo sia a livello sovranazionale, sia nella legislazione nazionale. Lo sforzo di questi ultimi anni è verso la costruzione di un perimetro di sicurezza che coinvolge tutte le strutture informatiche del Paese. Non a caso esso parte proprio dall'esperienza della Polizia postale e delle comunicazioni. La regolamentazione europea tenta di superare, con il *Digital Service Act* e il *Digital Market Act* la concezione proprietaria che i grandi operatori hanno dello spazio virtuale, passando così da un rapporto consensuale a uno di regolamentazione autoritativa, almeno parzialmente. In tale direzione dovrebbe andare anche l'*Artificial Intelligence Act*, in corso di redazione.

Parte essenziale della costruzione del perimetro di sicurezza è costituita dalla recente legislazione nazionale, che attraversa tutti i settori delle infrastrutture pubbliche e private e delle attività imprenditoriali e sociali, rendendo obbligatorie misure di sicurezza e l'attivazione di reazioni in caso di aggressione.

Centrale nella rete di protezione è la creazione della Agenzia Nazionale per la Ciber Sicurezza, della quale non a caso sono direttore e vice direttore due grandi esperti del settore, i prof. Roberto Baldoni e la nostra – permettetemi questa appropriazione – Nunzia Ciardi.

Inizialmente l'Agenzia era stata immaginata all'interno del DIS, quindi del Sistema per l'Informazione e la Sicurezza. Essa è ora resa autonoma, sia pure sempre nel riferimento al Presidente del Consiglio dei Ministri, responsabile della sicurezza nazionale, e pur continuando a far riferimento al DIS. Il perimetro della sicurezza, infatti, va oltre la sicurezza nazionale in senso stretto e richiede una serie di articolati interventi e contatti, che attraversano ogni aspetto della vita produttiva e sociale del Paese, dai trasporti alla sanità alle imprese.

Dunque, l'Italia si avvia verso un complesso sistema di protezione e – vedremo subito – reazione.

Il settore più delicato mi sembra tuttavia quello della cooperazione internazionale di polizia e giudiziaria. Siamo ancora molto lontani da una completa e universalmente accettata disciplina. Vi sono ancora visioni diverse tra grandi aree del mondo, dagli Stati Uniti e i Paesi anglofoni alla Russia e alla Cina. Anche in questo settore l'Europa si muove autonomamente, sia costruendo il concetto di prova digitale, sia operando verso il miglioramento della cooperazione internazionale, con molti strumenti, alcuni operativi come le strutture di polizia dedicate, altri normativi come la Convenzione di Budapest e il suo secondo protocollo aggiuntivo, aperto in questi mesi alla firma.

UNODC, l'organismo delle Nazioni Unite nel cui patrimonio è la Convenzione di Palermo, ha ben compreso che questa situazione costituisce una imperdibile opportunità per il crimine organizzato. La cifratura delle comunicazioni, già ora giunta a livelli elevatissimi, tanto da esser divenuta offerta commerciale, avrà presto le chiavi

inviolabili (se non forse attraverso le stesse enormi capacità di calcolo) del *Quantum Computing*. I mercati finanziari potranno essere oggetto di manovre speculative di non facile contrasto, sia attraverso la disinformazione (in forme più avanzate rispetto a quelle già sperimentate sulla manipolazione del mercato) che le grandi movimentazioni in ambiente virtuale. Ricatti, pedopornografia, riciclaggio e autoriciclaggio e tante tipologie di reati tradizionali saranno profondamente trasformati nella loro struttura dall'impiego di tecniche di IA. Ciò porterà a strutture organizzative della criminalità diverse da quelle a noi note, che potranno trarre esempio da quelle che in anni recenti hanno utilizzato il web per costituire associazioni con grande mobilità e che cercano di sfuggire allo schema associativo dei reati contro la personalità dello Stato.

Si tratta di reati prettamente transnazionali. Anzi, dovremmo dire sovranazionali. Essi si svolgono in larga parte in una realtà non identificabile con quella nota al diritto pubblico internazionale.

Lo spazio virtuale, o cyberspace, non è assimilabile a nessuna delle realtà sin qui note. Non è certamente corrispondente al territorio, cui è legato essenzialmente il concetto di sovranità nazionale, ma non può nemmeno essere ricondotto allo spazio siderale e alla sua disciplina internazionale. Lo spazio virtuale è in realtà strettamente legato ai territori, per la complessa rete materiale che consente L'immaterialità delle nuove tecnologie: dalle reti di comunicazione ai server fino alle strutture di produzione delle enormi quantità di energia che sono oggi necessarie per far funzionare i mega computer, che verrà ancora più incrementata dalla diffusione del *quantum computing*. Incidentalmente, le reti di comunicazione, come i cavi sottomarini o i ripetitori, sono altrettanto vulnerabili dei gasdotti, emersi quale obiettivo prioritario del complesso scenario della guerra in Ucraina. Questa relazione era stata già scritta quando si è verificato il grave "incidente" che ha isolato le isole Shetland.

Nonostante queste nette caratteristiche materiali, ciò che davvero caratterizza lo spazio virtuale è la immaterialità, la non localizzazione che da queste strutture materiali ha origine.

Questa dimensione appare avvicinarsi a quella dell'Alto Mare e dunque alla disciplina internazionale delle attività che in tale luogo si svolgono. Eppure lo spazio virtuale se ne differenzia radicalmente per la rigida divisione che anche questo ambiente misto conosce, tra dimensioni diverse, la terra, il mare, i fondali, le linee del territorialità e dunque della sovranità. E' questa sostanziale diversità che impedisce di estendere allo spazio virtuale l'esperienza che il nostro paese, a partire dalla procura di Catania, ha fatto nell'esercizio della giurisdizione anche a oltre 100 miglia dalla costa, applicando le convenzioni di Palermo (UNTOC) e sull'Alto Mare (Convenzione di Amburgo - SAR sul soccorso in mare – Londra – sicurezza della navigazione - e Montego Bay – diritto del mare).

Siamo così giunti al cuore del nostro problema: l'esercizio della giurisdizione. Si badi bene, non l'affermazione della giurisdizione nazionale. Questo può essere fatto da

qualunque Paese senza che ciò determini reazioni nella comunità internazionale. Vi sono Paesi che affermano, in alcuni ambiti, la propria giurisdizione universale, ad esempio in materia di crimini contro l'umanità. Anche la nostra legislazione conosce casi in cui si afferma la giurisdizione nazionale, utilizzando criteri diversi dalla territorialità. Tuttavia, ben differente è esercitare la giurisdizione. Compiere atti che costituiscono esercizio della giurisdizione, come indagini, perquisizioni, arresti, entra in diretto contrasto sia con regole del diritto pubblico internazionale, sia con l'affermazione della giurisdizione di altri Stati.

Questo espone non solo alla potenziale reazione dello Stato nella cui sovranità si pretende di attuare il nostro ordinamento. In realtà, l'esercizio di poteri al fuori delle attribuzioni potrebbe essere anche considerato come illecito dallo stesso ordinamento interno, esponendo chi pone in essere queste azioni (ad esempio arrestando un cittadino in un'altra Nazione, per poi portarlo in Italia) a responsabilità penale.

Tanto più che la recente giurisprudenza europea (Corte EDU e del Lussemburgo) considera rientrante nell'area della Convenzione e dei Trattati anche l'attività degli Stati e dei suoi agenti compiuta all'estero, quando in violazione di diritti fondamentali e manifestazione del concreto esercizio di sovranità.

D'altra parte, nel settore di cui ora ci occupiamo, la velocità nel seguire la traccia dell'attività illecita è essenziale per accertare il reato; e questa traccia conduce immediatamente a più Paesi, nella cui territorialità si basano reti e server e cloud. Un primo caso nel quale si è prospettata la responsabilità penale dell'agente ha riguardato proprio la Polizia postale e un magistrato della Procura di Roma, a lungo inquisiti prima che venisse esclusa l'illiceità della penetrazione in un server dal quale proveniva l'attacco informatico.

D'altra parte, la cooperazione giudiziaria è – anche nei casi migliori – di tale lentezza da essere di fatto incompatibile con le esigenze di accertamento del reato nello spazio virtuale (e di impedimento delle sue conseguenze, anch'esso dovere imposto alla polizia giudiziaria).

A questo tema, già di per sé tale da rendere difficile l'esercizio della giurisdizione nei casi di reati transnazionali commessi con l'impiego di tecnologie informatiche e avanzate, come è esperienza di chiunque abbia dovuto chiedere informazioni anche di assoluta semplicità al gestore di una piattaforma, si aggiunge il tema fondamentale della "attribuzione". Cioè della possibilità di affermare, sulla base di elementi di valutazione convincenti, che la condotta riprovevole possa essere attribuita a soggetti operanti nell'area territoriale di un altro Stato o comunque a tale sovranità soggetti.

Abbiamo più volte utilizzato il termine evidente, con riferimento al conflitto ucraino e alle acquisizioni circa la disinformazione o gli attacchi cibernetici. Lo abbiamo fatto consapevolmente per giungere a questo punto di svolta del nostro discorso.

Nello spazio virtuale nulla è evidente quanto ad attribuzione. Solo risalendo la catena delle innumerevoli azioni di macchine automatizzate, risiedenti materialmente in spazi di territorialità diversi, è possibile giungere fino a gangli riconoscibili e attribuibili a soggetti determinati. Ma tali attività si scontrano con la sovranità di Paesi, anche neutrali, cioè terzi rispetto agli attaccanti, attraverso i cui territori o comunque gli spazi su cui vi è rivendicazione di sovranità, come ad esempio il cloud, l'attacco è stato portato. Ciò che è necessario per impedire l'attacco, per evitarne gli effetti dannosi e infine per accertarne la provenienza è considerato illegale dal Paese straniero nel quale tali atti di accertamento devono essere svolti. Non si tratta del futuro, posto chi già si è concretizzato il rischio che tali attività, incidenti sulla sovranità di altri Paesi, siano considerate illecite anche nel nostro stesso Paese.

Queste difficoltà sono oggi affrontate nel campo della giustizia penale dal secondo protocollo aggiuntivo della convenzione di Budapest. Il protocollo è volto ad anticipare il consenso degli Stati coinvolti, attraverso la costituzione di squadre comuni stabili, non formate per singoli procedimenti. Si tratta però di un palliativo, non essendo stato raggiunto il consenso su di un meccanismo che legittimi l'attività di ingerenza nella giurisdizione, a determinate condizioni e salvo ratifica.

Problemi non diversi ci si trova ad affrontare nel campo delle relazioni tra Stati. È per questa ragione che è stato costituito presso le Nazioni Unite un gruppo di lavoro volto a definire il concetto di spazio virtuale, da cui discendono una serie di conseguenze.

L'italia ha presentato nel 2021 un *position paper* che afferma che anche lo spazio virtuale è soggetto al diritto pubblico internazionale e dunque anche al diritto umanitario internazionale. Ciò implica che si applicano allo spazio virtuale i principi che regolano le relazioni tra gli Stati nelle situazioni di conflitto o che possano portare al conflitto. Tali principi regolano la responsabilità degli Stati e le azioni che possono essere adottate sia per autodifesa sia ai fini della punizione di attività illecite provenienti direttamente da altri Stati oppure dai soggetti che tali stati hanno l'obbligo di controllare. Si ripropone qui il tema della attribuzione. Anche nel diritto umanitario internazionale le azioni di responsabilità e di autodifesa, fino al conflitto armato, richiedono l'attribuzione delle condotte illecite allo Stato aggressore o a soggetti che tale Stato avrebbe dovuto ostacolare (principio della *due diligence)*. Dunque, torniamo al punto di partenza. Al di là della attribuzione secondo criteri di carattere logico, ad esempio il criterio del *cui prodest* o l'individuazione di elementi meramente indizianti, ciò che dà certezza è in realtà la penetrazione dei sistemi informatici da cui proviene l'attacco. Tale strumento di accertamento è al tempo stesso il meccanismo di autodifesa e di attacco punitivo.

Tali complessi problemi vengono oggi affrontati dal decreto legge 9 agosto 2022, n. 115, convertito alla legge 21 settembre 2022, n. 142. Tale decreto attribuisce alle Agenzie di informazione il potere di tutelare il nostro Paese e le sue strutture da attacchi da qualunque parte provenienti, anche attraverso azioni difensive ed offensive.

Il presupposto di questa attribuzione di poteri è che gli attacchi pongano in questione la sicurezza nazionale. Al Sistema di informazione per la sicurezza, infatti, sono attribuiti soltanto i poteri che sono necessari per la tutela di questo valore fondamentale e non anche per altri, pur importanti, interessi costituzionali, come la repressione dei reati o la sicurezza pubblica. Si tratta, dunque, di un perimetro ben definito, sia in positivo che in negativo. In positivo, in quanto la sicurezza nazionale è fondata sui valori, individuati dalla Corte costituzionale nelle due sentenze in materia di segreto di Stato che sono alla radice della riforma del 1977 dei Servizi a Segreti, la n. 82 del 1976 e la n. 86 del 1977 e nei successivi conflitti di attribuzione tra poteri dello Stato, cioè tra l'autorità giudiziaria e la Presidenza del Consiglio dei Ministri.

I valori tutelati sono quelli che si riconducono allo Stato comunità e che danno vita alla repubblica democratica, nella sintesi dell'ordine costituzionale: dalla integrità del territorio e della sovranità, interna ed esterna, dello Stato, ai valori che in esso vivono, dai diritti fondamentali al metodo democratico, dal ripudio della violenza nello spazio pubblico al ripudio della guerra come strumento di risoluzione dei conflitti.

In negativo, in quanto mai i poteri attribuiti alle Agenzie potrebbero essere utilizzati per scopi di parte. La sicurezza nazionale è ben distinta dalle varie accezioni del termine sicurezza, tra cui quella pubblica. I grandi poteri attribuiti alle Agenzie non possono quindi essere utilizzati né per – altrimenti apprezzabili – fini di ordinaria prevenzione e tanto meno repressione di reati, neppure e tantomeno per finalità di parte, in danno di opposizioni o del dissenso.

Così delimitati dai confini costituzionali e dal diritto positivo (legge 124 del 2007 e successivi interventi in materia, in particolare legge 133 del 2012), le attività dei servizi segreti, comunque li si voglia definire, sono ricondotti allo Stato di diritto e portati a emersione dalle secche costituzionali della ragion di Stato.

Le Agenzie sono ora legittimate dal diritto positivo ad effettuare azioni difensive e offensive (sempre nei limiti del diritto pubblico internazionale), rispettando garanzie sostanziali e procedurali a tutela anche della responsabilità politica del Presidente del consiglio dinanzi al Parlamento, previste dagli artt. 17 e ss. della legge 124/2007, le c.d. garanzie funzionali.

A mio parere questi poteri erano già ricavabili dalla lettura sistematica delle attribuzioni del sistema di informazione per la sicurezza, quali desumibili dai principi costituzionali. In una materia così complessa e incerta è stato tuttavia utile l'intervento normativo che ha fatto definitiva chiarezza.

Residuano tuttavia problemi non secondari nella regolazione del rapporto tra gli interventi protettivi, attribuiti all'agenzia nazionale per la cyber sicurezza, quelli difensivi e offensivi attribuiti alle Agenzie di informazione e la funzione costituzionale di accertamento e punizione dei reati.

Le attività volte a contrastare immediatamente gli attacchi possono infatti determinare trasformazioni anche irreversibili nella sequenza delle attività contrastate, che tuttavia costituiscono parte di una condotta illecita il cui accertamento è devoluto all'autorità giudiziaria.

Questo problema non può essere affrontato in termini di primazia dell'accertamento penale, come forse un tempo si sarebbe fatto. Al contrario, i tempi strettissimi di reazione necessari per impedire che il danno si verifichi o si diffonda e al tempo stesso per accertare la provenienza dell'attacco, impongono una composizione dei diversi interessi. Questo implica, ad esempio, che sin d'ora dovrebbero essere utilizzati metodologie e protocolli in grado di attestare in maniera non modificabile ogni azione compiuta.

Siamo quindi di fronte a nuove sfide, certamente non irrisolvibili, ma che richiedono una consapevolezza dei problemi che abbiamo di fronte e che dobbiamo superare se vogliamo che la giurisdizione penale continui a svolgere la sua funzione anche nello spazio virtuale.

Non si tratta di rivendicare una funzione che si afferma essenziale. Comprendo bene che vi sono situazioni e momenti in cui anche l'accertamento penale può essere considerato recessivo rispetto alla tutela della sicurezza nazionale. La preoccupazione che credo ci debba guidare è di altro genere.

L'accertamento penale si basa infatti, per sua stessa natura e per le garanzie in cui si invera, che sono garanzie per l'imputato ma al tempo stesso di verità dell'accertamento, sulla trasparenza delle procedure e sulla controllabilità degli esiti a cui queste pervengono. Le azioni, pur legittime e anzi doverose, che si svolgono nello spazio delle attività di contrasto di minacce tra Stati, sono invece basate sul principio della segretezza, anche questo del tutto legittimo. Azioni condotte in questo terreno e con tali modalità comportano però il rischio di reazioni analoghe e dunque di una progressione incontrollabile.

Una ragione di più per operare fattivamente nelle sedi internazionali, delle Nazioni Unite, dell'Unione Europea e del Consiglio d'Europa, per un'efficace disciplina della giurisdizione penale nello spazio virtuale. Forse andrebbe anche affrontato con maggiore determinazione il tema del rapporto tra la tutela della riservatezza e gli accertamenti che possono essere condotti ai fini della giustizia penale e della sicurezza nazionale, aspetti a volte collegati ma che debbono essere tenuti ben distinti.

Di grande utilità sono le strutture che si vanno costituendo a livello europeo, anche con funzioni di intelligence e giudiziarie, finalizzate all'accertamento di reati transnazionali commessi nello spazio virtuale.

Anche dal punto di vista della legislazione interna qualcosa può già essere fatto per adeguare gli strumenti sostanziali e processuali alle nuove dimensioni dei reati

commessi nello spazio virtuale. La soluzione non è nel conflitto tra poteri, nuovamente dietro l'angolo quando l'esigenza di accertamento si scontrerà con quella della prevenzione, ma nella loro chiara regolazione normativa.

Ciò che, a mio parere, è di assoluta, prioritaria necessità è che si diffonda tra la magistratura, anche giudicante, e tra le Forze di polizia la consapevolezza della complessità di questi temi e che si consolidi la necessaria formazione professionale.