Prof. Avv. Ranieri Razzante

C.R.S.T
Centro di Ricerca sulla Sicurezza ed il Terrorismo

Commissioni riunite, I Commissione Affari Costituzionali e II Commissione Giustizia, Camera dei Deputati

Audizione del Prof. Ranieri Razzante nell'ambito dell'esame del disegno di legge A1717, recante "*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*"

Egregi Presidenti, *Onorevoli Deputati*,
ringrazio per l'invito a scrivere questo contributo sul disegno di legge A1717 in materia di rafforzamento della *cybersicurezza*. È un onore per me redigere il presente scritto al fine di porre l'attenzione su alcune tematiche, quali le *cybermafie*, il *cyberterrorismo*, il ruolo centrale oramai occupato dall'Intelligenza Artificiale (IA) e i risvolti in ambito penale, soprattutto in tema di investigazioni e di attribuzione di responsabilità, così da consentire riflessioni utili ai fini di redigere la versione finale del disegno di legge di cui trattasi.
In particolare, si intende sottoporre al vaglio parlamentare alcuni spunti di riflessione circa la necessità di garantire la certezza del diritto e il rispetto dei diritti fondamentali. A ben vedere, infatti, Internet è divenuto il *locus commissi delicti* preferito dalle associazioni criminali, in particolare di stampo mafioso e terroristico. In questo scenario, stante l'esigenza preminente di individuare un quadro normativo di riferimento, il disegno di legge di cui si discute rappresenterà una pietra miliare e un punto di partenza (*non certo di arrivo*), e si porrà in linea con lo scenario europeo, tenuto conto del *Cyber Resilience Act*, approvato dal Parlamento europeo il 12 marzo 2024, e trasmesso per l'approvazione formale al Consiglio Europeo per diventare legge nelle prossime settimane.

Le cybermafie e i modelli della criminalità informatica organizzata

La nozione di criminalità informatica è piuttosto recente, e purtuttavia ha già avuto una significativa evoluzione. Per comprendere al meglio la questione è necessario, anzitutto, definire cosa debba intendersi per reati informatici, anche detti *cybercrimes*, e, in generale, approfondire il concetto di criminalità informatica organizzata.
I primi consistono in comportamenti illeciti in cui il soggetto attivo, c.d. *hacker*, pone in essere una condotta antigiuridica che ha come obiettivo alterare e/o danneggiare il sistema informatico altrui. Quest'ultimo è stato indicato dall'art. 1 della Convenzione europea di Budapest del 23 novembre 2001 come «qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica dei dati». Dal momento che un apparato elettronico può elaborare un elevato numero di dati ed informazioni, la pirateria informatica può ledere molteplici beni giuridici che siano di natura privata o pubblica.
Con la crescita esponenziale di tali infrazioni, si è assistito all'aumento della criminalità informatica organizzata, che si contraddistingue per l'esistenza di un rapporto stabile e duraturo tra i suoi componenti, i quali fondano un'associazione per delinquere. Per *gruppo organizzato* si intende un insieme di persone che agiscono di comune accordo, tramite una struttura ordinata gerarchicamente, che viene a costituirsi al fine di commettere uno o più reati.

Via Guidubaldo del Monte, 13 - 00197 Roma Tel 06 8417399
razzante@iusconsulting.it www.ranierirazzante.it

Lo scopo finale è quello di ottenere, direttamente oppure indirettamente, vantaggi finanziari o materiali. Le organizzazioni in questione, operando all'interno del *network*, hanno una capacità offensiva sovranazionale.
È fondamentale, dunque, adeguare gli strumenti tecnologici alle nuove sfide nel contrasto alla criminalità organizzata, nonché aumentare le capacità di penetrazione nel Metaverso e nel *dark web*.
I criminali moderni sfruttano, come detto, la tecnologia per arrivare direttamente alle "vittime" che, il più delle volte, vertono in una condizione di inconsapevolezza e, perciò stesso, di debolezza. La migliore arma, in tal caso, oltre ad una buona base normativa, è l'informazione: divulgare indicazioni affinché vi sia maggior consapevolezza dei rischi e delle conseguenze sanzionatorie. Il rischio, per l'utente non informato, è quello di accedere al *dark web* – azione che di per sè non è illegale – e trovarsi in quel sottobosco che è teatro di una serie di attività criminose, dal contrabbando e lo spaccio di droga, al riciclaggio e la pirateria, fino all'usura e la violenza.
È sempre più frequente l'uso dei *social network* da parte delle organizzazioni mafiose per condividere messaggi testuali e frammenti audiovisivi espliciti di ispirazione "clanistica". Strumenti quali *Whatsapp*, *Youtube*, *Tik Tok*, *Instagram*, *Twitter*, *Facebook*, sono ormai serbatoi potenziali di informazione criminale: lo scopo del loro utilizzo è, certamente, quello di servirsi di mezzi che, in modo rapido e diretto, permettano di comunicare, affermarsi ed espandersi, nonché di veicolare specifiche informazioni ai giovani, ovvero nei soggetti più facilmente influenzabili.
Risulta evidente, quindi, come la comunicazione attraverso i *social* acquisisca un ruolo centrale nella prevenzione dell'affiliazione dei giovani. Ad oggi, il miglior investimento per prevenire e contrastare le mafie è ancora quello sull'educazione. Tale sfida educativa deve essere più forte nelle aree dove si concentra la povertà minorile e dove, di conseguenza, si accentuano le disuguaglianze sociali. Invero, tra le principali componenti dell'affiliazione dei giovani vi sono l'indebolimento dei legami sociali, la disorganizzazione sociale, l'adesione alle subculture devianti, il conflitto fra culture, le forme di etichettamento e il ruolo delle agenzie del controllo sociale, la frustrazione di *status*, la correlazione positiva tra marginalità sociale e devianza, la disgregazione e basso controllo familiare, il coinvolgimento in attività illecite come soluzione ai bassi rendimenti delle attività lecite e la minore allocazione del tempo individuale in opportunità legali. Tra queste si ritrovano, tuttavia, ulteriori elementi, quali: il *deficit* di sorveglianza e di controllo sociale, lo sviluppo e la diffusione delle organizzazioni criminali, la formazione di una struttura illegittima di opportunità, la reattività alla marginalità e alle diverse forme di esclusione sociale e, infine, carriere criminali scelte come opzioni di vita più vantaggiose. Questi sono un evidente campanello d'allarme, poiché, evidenziano non solo una necessità di interventi educativi, bensì un doveroso intervento dello Stato nel controllo e nella sorveglianza, *online* e non, al fine di ridurre e di prevenire l'accrescere dell'interesse verso realtà criminali nei giovani.
Può osservarsi che il fenomeno, particolarmente critico e di risonanza internazionale, della criminalità informatica organizzata ha assunto un rilievo giuridico tale da divenire oggetto di competenza penale dell'Unione europea, *ex* art. 83, par. 1, TFUE.
In primo luogo, è necessario osservare che si delinea una varietà di reati commessi da associazioni per delinquere come anche da strutture differenti. Talvolta, il modello di organizzazione è contraddistinto da una singola componente, come nelle aggregazioni familiari o di tipo mafioso; in altri casi, l'elemento tipico di una struttura si combina con requisiti comuni ad altri modelli. Ma vi

Via Guidubaldo del Monte, 13 - 00197 Roma Tel 06 8417399
razzante@iusconsulting.it www.ranierirazzante.it

è di più. I membri stabili di una determinata attività criminale possono essere affiancati da persone fisiche o giuridiche che offrono un apporto sporadico alla commissione degli illeciti. Pertanto, nei reati più "*complessi*", è necessaria l'integrazione di ruoli distinti e ciò determina la diffusione di una molteplicità di modelli; l'esigenza di una vasta gamma di funzioni per eseguire un reato "*complesso*", però, non implica necessariamente anche la complessità strutturale del gruppo criminale: spesso una rete delittuosa è composta non da singoli individui bensì da alleanze ben ordinate ed organizzate.
Sebbene sia un tentativo arduo classificare tali organismi, i rapporti fra crimine organizzato e crimine informatico si possono interpretare seguendo tre schemi: *a*) la criminalità organizzata, definita tradizionale, può servirsi delle nuove tecnologie o di Internet – compresi *deepweb* e *darknet* – per commettere reati o per realizzare attività preparatorie (come comunicazioni protette fra i membri dell'organizzazione ovvero per investire e/o occultare proventi di origine delittuosa o le tracce del reato); *b*) la criminalità organizzata tradizionale si può avvalere, inoltre, dei servizi offerti da singoli professionisti esperti o da molteplici malviventi associati, che operano nel *web* e, soprattutto, nel *deepweb*. Tra queste, a titolo esemplificativo e non esaustivo, possono citarsi la compravendita di identità digitali o di nuovi documenti di identità; lo spionaggio o l'acquisizione di informazioni attraverso accessi illeciti a sistemi informatici; il monitoraggio dell'attività di determinate persone o enti tramite l'uso di *software* installati in qualsiasi *device*, come *smartphone*, *tablet*, *laptop*; il danneggiamento di sistemi informatici o di dati e di informazioni *ivi* archiviate, l'acquisizione di sistemi o piattaforme per realizzare frodi, commettere reati economici o *cyber laundering* e sfruttare le risorse del gioco d'azzardo *online*, comprese le scommesse clandestine *etc.*; c) il c.d. *Cyber Organized Crime* (COC), ossia il crimine informatico organizzato: si tratta di congregazioni che operano nel *cyberspace* e che realizzano reati informatici oppure offrono servizi a singoli o a gruppi criminali (*crime as a service*). Qui, struttura ed organizzazione sono strettamente legate alla tecnologia e, in questo modo, tali soggetti si garantiscono la sopravvivenza, realizzando frodi o reati economici (anche tramite accessi non autorizzati a sistemi informatici o furti di identità), sfruttando le risorse del gioco d'azzardo *online*, offrendo le proprie professionalità e stringendo legami con organizzazioni criminali tradizionali e, persino, terroristiche. Quest'ultimo modello è di nuova generazione, pertanto, pur essendo un'organizzazione costituita da persone, sfugge alle tradizionali definizioni di crimine organizzato.

Il cyberterrorismo
Vista l'assenza di confini geografici e la possibilità di colpire beni di qualsiasi natura – privata e pubblica – attraverso la rete, si è diffuso il fenomeno del c.d. *cyberterrorismo*, una recente evoluzione del terrorismo che segna l'avvio di un nuovo capitolo della storia mondiale. Il *cyberterrorismo* presenta un problema definitorio. Questa lacuna deriva, a monte, dall'incertezza nell'inquadrare il fenomeno già da un punto di vista fattuale e reale. Il dibattito in merito alla questione terminologica si amplia se si tiene conto dei pareri degli esperti: alcuni di essi negano azioni di *cyberterrorismo*, mentre altri ritengono che alcuni gruppi ricorrano sistematicamente alla rete.
È indubbio come la stessa società dell'era digitale, impiegando la tecnologia informatica e telematica in settori sempre più ampi, abbia consentito ai gruppi terroristici di poter accedere con maggiore facilità alle informazioni circa le cc.dd. *infrastrutture critiche*, quali sistemi di difesa nazionali, sistemi

di controllo e di trasporto di persone e merci, sistemi di controllo di fonti energetiche, sistemi sanitari e circuiti economico-finanziari.
Il c.d. *cyberterrorismo*, quindi, è una particolare declinazione del terrorismo tradizionale, che ha cambiato la natura e le modalità delle minacce alla sicurezza internazionale, rendendole più dinamiche e fluide rispetto al passato.
In tale contesto, la rete figura in ogni aspetto dell'organizzazione criminale e diviene essenziale per attività quali il reclutamento, il finanziamento e la propaganda.
In aggiunta, la rete svolge un ruolo primario nel mantenimento e nell'operatività delle organizzazioni criminali: dalla commistione tra il terrorismo e gli strumenti informatici nasce un nuovo pericolo, smaterializzato, delocalizzato e, spesso, imprevedibile.
L'ambiente *online* è un mezzo fondamentale per la propaganda terroristica e le forze dell'ordine osservano una diversificazione dei temi nelle discussioni *online* che vengono ripresi in narrazioni terroristiche. Ciò abbassa ulteriormente la soglia di ingresso nel mondo dell'estremismo violento e del terrorismo, amplia la gamma di individui che possono facilmente essere esposti alla radicalizzazione e aumenta la volatilità e l'imprevedibilità della scena dell'estremismo violento e dello stesso terrorismo. Inoltre, lo stesso ambiente online garantisce la durata del materiale di propaganda, che rimane accessibile a potenziali nuove reclute.
I domini web emergenti, come il Metaverso, potrebbero essere utilizzati per la diffusione della propaganda, il reclutamento e il coordinamento delle attività terroristiche e di estremismo violento. Uno sviluppo simile potrebbe essere osservato con le piattaforme decentralizzate *open source*, che stanno diventando sempre più popolari tra i terroristi e gli estremisti violenti.
In futuro, i terroristi potrebbero mostrare un interesse crescente per le armi tecnologicamente avanzate o abilitate. Si prevede che tali armi diventino sempre più accessibili, scambiate *online* in forma anonima o fornite da attori criminali. I droni e altri tipi di dispositivi e veicoli senza pilota consentirebbero ai terroristi di perpetrare attacchi a distanza, amplificandone l'impatto. I veicoli senza pilota possono anche essere personalizzati e utilizzati in combinazione con varie armi, potenzialmente anche radioattive o biologiche.
Ispirato dalle narrazioni sulla pandemia e con le prossime scoperte nel campo della biologia sintetica e delle biotecnologie, il passaggio al *bioterrorismo* potrebbe diventare più pronunciato in futuro. Tra le tante, l'*Internet degli oggetti* (IoT) e l'*Intelligenza Artificiale* (AI), anche sotto forma di *deep fake*, realtà aumentata e AI conversazionale, sono sfaccettature della tecnologia che si prevede saranno utilizzate più spesso dai terroristi, compresi quelli che operano o pianificano attacchi nell'UE. Tali strumenti possono essere utilizzati per migliorare l'efficienza della propaganda e accelerare la radicalizzazione *online*, nonché per compiti più pratici come il funzionamento a distanza di veicoli e armi utilizzati negli attacchi o la creazione di campi di addestramento virtuali, accessibili a un pubblico illimitato in tutto il mondo. I terroristi potrebbero utilizzare sempre più spesso valute e piattaforme digitali per spostare virtualmente i fondi. Ci sono già stati segnali di sperimentazione o utilizzo di NFTs per ottenere fondi per il finanziamento del terrorismo, a dimostrazione del fatto che i terroristi stanno esplorando le opportunità offerte dai progressi digitali e tecnologici. Allo stesso modo, i terroristi potrebbero utilizzare metodi più sofisticati e a più livelli per raccogliere, spostare e nascondere i fondi utilizzati per sostenere le loro organizzazioni e operazioni.

Via Guidubaldo del Monte, 13 - 00197 Roma Tel 06 8417399
razzante@iusconsulting.it www.ranierirazzante.it

A fronte della natura peculiare del fenomeno *de quo*, è utile analizzare gli strumenti approntati dal Legislatore, nazionale e sovranazionale. In un ambito in cui è necessario attuare una tutela preventivo-repressiva, si concretizza il rischio di una risposta legislativa, sostanziale e processuale, non conforme ai principi costituzionali di riserva di legge, offensività e giusto processo, *ex* artt. 25 comma 2, 111 Cost. e artt. 6 e 7 CEDU, per un duplice ordine di ragioni: l'inadeguatezza dei sistemi di difesa informatici statali e la natura ibrida del fenomeno terroristico e *cyberterroristico*, che rende necessario trovare una sintesi tra discipline giuridiche ed *extra*-giuridiche.
Sul piano del diritto penale sostanziale ancora non è stata prevista una fattispecie unitaria che tipizzi il terrorismo *cibernetico*, fenomeno che presenta denominatori comuni alla criminalità informatica e al terrorismo tradizionale. Questa convergenza è evidente negli attacchi informatici a motivazione politica, attuati con la finalità di cagionare gravi e, spesso irreversibili, danni all'istituzioni, all'economia, alla vita e all'integrità fisica.

L'IA valorizza e non sostituisce l'intelligenza umana. Profili penali.
L'IA è indubbiamente una delle tecnologie emergenti più promettenti del nostro tempo. Strumento dall'enorme potenziale, è in grado di migliorare la nostra efficienza, di incrementare la produttività, nonché di rivoluzionare la nostra vita quotidiana.
Secondo la definizione fornita nella Comunicazione della Commissione europea del 2018 (*Communication Artificial Intelligence for Europe*), l'AI si riferisce a sistemi che mostrano un comportamento intelligente, che sanno analizzare il loro ambiente e agire – con un certo grado di autonomia – per raggiungere obiettivi specifici.
In altre parole, l'IA consiste nell'abilità di una macchina di mostrare capacità umane quali l'apprendimento, il ragionamento, la creatività e la pianificazione: si tratta, quindi, di sistemi intelligenti, in grado di adattare il loro comportamento sulla base degli effetti delle azioni precedentemente inoculate. In particolare, le capacità tipiche dell'essere umano, riguardanti la comprensione e l'elaborazione del linguaggio naturale (NLP – *Natural Language Processing*) e delle immagini (*Image Processing*), vengono in qualche modo "*sintetizzate*" nell'IA. Ciò avviene tramite la ricezione di dati, preparati e raccolti mediante sensori da parte di un computer che, una volta processati, risponde lavorando in autonomia.
La preminente esigenza di avere un quadro normativo di riferimento per disciplinare la tematica complessa dell'intelligenza artificiale, se in ambito nazionale sarà parzialmente garantita dal disegno di legge di cui trattasi, in ambito europeo è affidata all'AI Act, regolamento che, a tre anni dalla proposta – datata 21 aprile 2021 – è (finalmente) entrato in vigore il 13 marzo 2024, consentendo all'Europa di essere pioniera e apripista nel panorama mondiale.
A ben vedere, l'IA è una realtà che si sta sviluppando sempre più velocemente e che già sta avendo un grande impatto sul modo di vivere delle persone. Visti i grandi cambiamenti tecnologici in corso e le possibili nuove sfide, l'UE si impegna, mediante un intervento legislativo che assicuri il buon funzionamento del mercato interno, affinché sia i benefici che i rischi legati all'uso dei sistemi di IA siano affrontati e distribuiti in modo adeguato a livello europeo. Pertanto, l'obiettivo principale è quello di sviluppare un'IA sicura, etica ed affidabile, dove per IA deve intendersi, *ex* art. 3 del Regolamento AI: «*Un sistema basato su macchine progettato per operare con vari livelli di autonomia e che può mostrare adattabilità dopo il dispiegamento e che, per obiettivi espliciti o impliciti, deduce dagli input ricevuti come*

Via Guidubaldo del Monte, 13 - 00197 Roma Tel 06 8417399
razzante@iusconsulting.it www.ranierirazzante.it

generare output quali previsioni, raccomandazioni di contenuti o decisioni che possono influenzare ambienti fisici o virtuali».

Nonostante le più recenti evoluzioni tecnologiche e normative e la circostanza che l'IA sia uno strumento in grado di apportare un grande valore aggiunto in molti ambiti di vita, non si tratta di una sostituzione all'*intelligenza umana*. Invero, occorre ribadire che essa nasce per essere a supporto e a servizio dell'umanità, per orientare quest'ultima nella gestione delle situazioni complesse. Per tale ragione, in riferimento all'ambito penale, sarebbe irragionevole non sfruttare il grande apporto che tale strumento può fornire: basti pensare ai nuovi *software* informatici, agli algoritmi predittivi sull'esito delle controversie, all'apporto della robotica e della logica dell'IA.

In tema di diritto penale e, in particolare, di indagini ed investigazioni, merita qualche riflessione il ruolo che l'AI Act riconosce alle forze dell'ordine nella fase delle indagini. Infatti, in tema di c.d. polizia predittiva, può dirsi che il Regolamento AI, all'art. 26 - recante *Obblighi dei deployer dei sistemi di IA ad alto rischio* - esclude le applicazioni di IA che potenzialmente possano costituire una minaccia per la salvaguardia dei diritti fondamentali, quali, a titolo esemplificativo, sistemi di categorizzazione biometrica. In particolare, l'art. 26, comma 2, precisa che: «I *deployer* affidano la sorveglianza umana a persone fisiche che dispongono della competenza, della formazione e dell'autorità necessarie nonché del sostegno necessario». Degno di nota è il comma 10 del medesimo articolo, secondo cui :«*Fatta salva la Direttiva 2016/680/UE, nel quadro di un'indagine per la* ***ricerca mirata di una persona sospettata o condannata per aver commesso un reato****, il deployer di un sistema di IA ad alto rischio per l'identificazione biometrica remota a posteriori chiede un'****autorizzazione, ex ante o senza indebito ritardo ed entro 48 ore, da parte di un'autorità giudiziaria o amministrativa*** *la cui decisione è vincolante e soggetta a controllo giurisdizionale, per l'uso di tale sistema, tranne quando è utilizzato per l'identificazione iniziale di un potenziale sospetto sulla base di fatti oggettivi e verificabili direttamente connessi al reato.* ***Ogni uso è limitato a quanto strettamente necessario per le indagini su uno specifico reato****. Se l'autorizzazione richiesta di cui al primo comma è respinta, l'uso del sistema di identificazione biometrica remota a posteriori collegato a tale autorizzazione richiesta è interrotto con effetto immediato e i dati personali connessi all'uso del sistema di IA ad alto rischio per il quale è stata richiesta l'autorizzazione sono cancellati*». Pertanto, le forze dell'ordine non potranno far ricorso ai sistemi indicati, salvi i casi previsti dalla legge; inoltre, per l'identificazione in tempo reale, si renderà necessario un limite spaziale e temporale, oltre ad una autorizzazione giudiziaria o amministrativa. In termini concreti, gli utilizzi consentiti potrebbero includere le ricerche per individuare persone scomparse o per prevenire attacchi e cyberattacchi di matrice terroristica ed eversiva. Si tratta di utilizzi considerati "*ad alto rischio*" per i quali il legislatore europeo ha previsto che vi sia la connessione con un reato.

Si rende necessario, in tale scenario, (*ri*)considerare il rapporto tra IA e Diritto Penale, seppure con le dovute precauzioni: occorre ribadire che le qualità umane non potranno mai essere totalmente sostituite dalla tecnologia, visti anche i rischi che il sistema di giustizia penale dovrà affrontare, ma si auspica il mantenimento di un modello che persegua l'obiettivo primario di una "*giustizia giusta*", non rinunciando all'apporto del progresso tecnologico.

L'IA aspira a subentrare nel sistema penale in svariati ambiti, quali il *policing*, il *profiling* e il *sentencing*, sfidando, al contempo, il "*fattore umano*". Si auspica che anche nel sistema penale italiano l'utilizzo di tale tecnologia rappresenti un'arma efficace ed efficiente nella prevenzione e repressione dei

Via Guidubaldo del Monte, 13 - 00197 Roma Tel 06 8417399
razzante@iusconsulting.it www.ranierirazzante.it

reati, fornendo la desiderata tutela dei beni giuridici. Tuttavia, gli eventuali vantaggi sono connessi a probabili rischi inerenti all'etica e ai diritti fondamentali. A tal proposito, si prospettano diverse proposte, sia in sede investigativa sia in sede giudiziaria.
In primo luogo, si pensi al miglioramento delle risorse di *law enforcement* e, di conseguenza, delle attività di *policing* e di *profiling* che permetterebbero di "*mappare*" il rischio criminale, al fine di ridurre la commissione di reati prevedibili e di individuare con maggior precisione i responsabili dei crimini.
In secondo luogo, in sede giudiziale, si ragiona sulla maggior precisione delle valutazioni mediante algoritmi predittivi; si tratta di strumenti che analizzano un numero elevato di dati del passato e individuano delle ricorrenze. Si pensi alla pericolosità di un soggetto condannato, che rileva: *a*) per il rischio di recidiva; *b*) per l'applicazione o la revisione di una misura di sicurezza; *c*) per commisurare la pena secondo gli indici individuati dall'art. 133 c.p.; *d*) per l'applicabilità della sospensione condizionale della pena; *e*) per la concessione di benefici penitenziari e l'applicazione di misure alternative alla detenzione; *f*) per l'applicazione della misura di prevenzione della sorveglianza speciale di pubblica sicurezza.
A tal proposito, nell'ordinamento italiano si avverte sempre di più la mancanza di certezza del diritto penale e ciò alimenta l'interesse verso il progresso e le innovative proposte dell'IA. Ciononostante, allo stato dei fatti, vi sono diversi problemi da fronteggiare, *in primis* quello delle garanzie fondamentali e della compatibilità costituzionale.
Nello specifico, l'utilizzo degli algoritmi renderebbe difficile il rispetto del principio di eguaglianza, sancito dall'art. 3 Cost.; invero, gli algoritmi sono, di per sé, non egualitari, dal momento che non considerano i fattori di rischio – come età, genere, luogo di residenza, *background* socioeconomico, abitudini di vita – nella loro totalità. Ne discende che i risultati offerti alle Autorità competenti risultino poco esaustivi e non completi.
Altra problematica che può evidenziarsi riguarda il rispetto del principio democratico e di trasparenza, poiché l'algoritmo si affianca ed integra la legge. In aggiunta, vi è il rischio di una modifica della cornice culturale in relazione all'offensività del reato, nonché alla personalità della responsabilità penale, sancita dall'art. 27 Cost.: difatti, si corre il pericolo di generalizzazioni statistiche che allontanano dalla valutazione del fatto concreto, tendendo a standardizzare un prototipo di criminale sulla base di decisioni pregresse.
Per altro versante, rileva il rischio che non si rispetti il principio del giusto processo e la relativa tutela del diritto di difesa: difatti, può evidenziarsi la possibilità di falsificazione dei dati elaborati dall'algoritmo e, di conseguenza, la dubbiosa affidabilità dello stesso.
Da ultimo, sempre correlato al diritto *ex* art. 24 Cost., si attenziona il concetto dell'analisi algoritmica dei dati e il diritto al silenzio dell'imputato: i dati risultanti dagli algoritmi possono creare problematiche legate all'uso di determinate informazioni desunte poiché andrebbero contro il diritto secolare riconosciuto all'imputato, ovvero il diritto di difendersi tacendo. Invero, il processo penale riconosce all'imputato un pieno diritto al silenzio in ordine alla propria responsabilità.
È chiaro che tali problematiche non devono causare una chiusura totale verso il progresso, poiché è indubbio l'apporto positivo dell'IA nell'ordinamento penale italiano – soprattutto in questo momento storico. Al contrario, dovrebbe mostrarsi un atteggiamento propositivo verso il progresso, tenendo conto che non è possibile stravolgere l'impianto penalistico italiano nel tentativo di "*correre dietro*" l'IA: la storia insegna che la tecnologia e il progresso non vanno di pari

Via Guidubaldo del Monte, 13 - 00197 Roma Tel 06 8417399
razzante@iusconsulting.it www.ranierirazzante.it

passo con il diritto, prova ne è la sempre crescente importanza acquisita dal diritto vivente e sarebbe irragionevole stravolgere tale dinamica. In conclusione, si auspica un utilizzo razionale ed un impiego efficiente dell'IA, nel rispetto dei principi che permeano il diritto penale, sostanziale e processuale, e dei diritti fondamentali sanciti dalla Costituzione e dalle Carte sovranazionali.
Tali considerazioni vanno inoltre a confluire nella "cybersecurity dell'IA e con la IA", della quale il ddl in esame dovrebbe, secondo chi scrive, tenere conto.

Algoritmi predittivi, attribuzione di responsabilità e intercettazioni
Il fenomeno dell'IA è ormai diventato un tratto distintivo della società odierna: si presenta come l'ultima frontiera del processo tecnologico e si diffonde in molti aspetti della vita quotidiana. Per tale ragione, viene in rilievo il rapporto tra IA e giudizio penale, che investe gran parte del paradigma processuale.
La diffusione di modelli basati sull'IA sta producendo un forte impatto sulla sfera decisionale, con particolare riguardo alle nuove frontiere della prevedibilità giuridica e dei *risk assessments* per il calcolo del rischio individuale. L'utilizzo di tali tecnologie in ambito giudiziario comporta una riflessione che faccia leva sulle principali criticità; inoltre, il contesto processuale comporta una forte tensione alla cornice costituzionale delle tutele, soprattutto in riferimento al "*potere decisionale artificiale*". Invero, il ricorso e l'utilizzo di algoritmi, se non assistito da requisiti di accessibilità e trasparenza, rischia di produrre un "*buco nero giuridico*" in cui la decisione risulti difficile: l'uso di prove algoritmiche può porre problemi riguardo il rispetto del principio del contraddittorio, in modo da sacrificare la dialettica processuale per un deficit di "*trasparenza probatoria*".
In tale contesto, l'ambito della prevenzione è quello che ha maggiormente interessato soluzioni basate sull'IA: la prevenzione si basa sulla connessione di vari elementi che possono suggerire previsioni sulla commissione di reati, in modo da consentire l'intervento di *law enforcement*.
Risulta evidente come gli applicativi informatici siano in grado di realizzare un'analisi più efficiente rispetto alle persone fisiche e di ottimizzare risorse e mezzi, poiché si tratta di sistemi in grado di realizzare immagini e video per prevedere le zone a più alto rischio criminale e individuare soggetti potenzialmente pericolosi. Anche nel campo dei social *network* l'impiego di algoritmi predittivi risulta molto utile nella localizzazione di possibili reati: difatti, l'algoritmo è in grado di realizzare una "*mappa*" di alcune aree connesse alla commissione di vari tipi di delitti, elaborando un risultato che favorisce l'intervento della polizia.
Tuttavia, gli algoritmi non esauriscono la propria collocazione solo in queste fasi, ma sono destinati ad applicazioni che riguardano anche il momento "*decisorio*". L'elemento di connessione tra la decisione umana e quella robotica è da rintracciare nello sforzo della disciplina processual-penalistica verso una oggettivizzazione della giustizia che riguarda la necessità di garantire una decisione che sia la più possibile equa, razionale ed imparziale.
In aggiunta, il concetto di prevedibilità va letto sia come necessità di poter prevedere le conseguenze delle proprie azioni (diretta espressione del principio di legalità *ex* art. 25 Cost.), sia nella possibilità di avere contezza dell'esito di un processo: una piena attuazione del principio implica che ciascun soggetto deve essere messo nella posizione di sapere cosa aspettarsi dall'apparato giudiziario, soprattutto per capire a quali conseguenze andrà incontro.

Via Guidubaldo del Monte, 13 - 00197 Roma Tel 06 8417399
razzante@iusconsulting.it www.ranierirazzante.it

La calcolabilità diviene l'obiettivo del sistema giuridico, declinabile anche in termini di prevedibilità di eventi umani. In questo caso la prevedibilità misura il grado di effettività delle norme che "impongono comportamenti ad esse conformi e sanzioni comportamenti ad esse difformi". Facendo riferimento al sistema penale, i casi principali riguardano le situazioni in cui il giudice deve compiere una valutazione sulla condotta futura di un soggetto e sulla sua pericolosità sociale.
L'ambito applicativo dell'accertamento penale deve essere circoscritto ad una serie di regole proprie del nostro ordinamento: un importante punto di riferimento è l'insieme di regole ricavate dall'art. 111 Cost., che costituisce gli argini per l'espletamento di un giusto processo, che si propone di tutelare la funzione cognitiva quanto i diritti dell'accusato.
Sul piano dell'accertamento, una svolta è derivata dall'evoluzione del sapere scientifico, messo a servizio dell'ambito probatorio attraverso mezzi di prova, tuttavia, in merito, emergono molteplici criticità. In generale, l'avanzare dell'IA vede l'aumentare delle problematicità nell'intero ambito della giustizia penale. Difatti, si assiste ad una vera e propria rivoluzione giuridica che sta attraversando tutti i settori del diritto e che si lega inevitabilmente ad una "*frattura antropologica*". Il sistema penale, seppur controllabile secondo determinati criteri, risulta essere fallibile poiché si struttura attorno alla persona. In prima istanza, è edificato sull'uomo: basti pensare alla responsabilità personale in conseguenza di una azione umana; in seconda istanza, è giudicato dall'uomo stesso: difatti, il processo penale è affidato ad un giudice e basato sulla sua capacità di comprensione e di valutazione. Lo strumento di controllo di tale discrezionalità è la motivazione, fondata su ragionevolezza e fondatezza delle argomentazioni che, anche quando vi è interpretazione, deve essere sorretta da un fondamento ermeneutico controllabile.
Già in precedenza, il sistema penale si è scontrato con la complessa tematica della responsabilità penale derivante da una condotta non imputabile ad un essere umano, che ha condotto all'incriminazione delle persone giuridiche – "*entità inumane*" – grazie al D. Lgs. n. 231 del 2001. L'ingresso dell'IA, quindi, apre un nuovo scenario poiché il diritto penale si dovrà confrontare con macchine *self-driving*, per le quali sarà necessario discutere ampiamente in merito all'imputazione della responsabilità a seguito della causazione di reati.
Ciò comporta diverse difficoltà. In primo luogo, si propongono dubbi giuridici. Invero, ci si chiede se gli attuali moduli di attribuzione della responsabilità penale possano adattarsi a casi di condotta realizzata in maniera condivisa da IA ed essere umano, ovvero ad un fatto-reato posto in essere da una macchina solo "assistita" dalla presenza umana inerte ed eventuale.
Dunque, il dilemma che rileva è a chi debba imputarsi un evento colposo: a chi ha generato il focolaio di rischio ideando l'algoritmo; a chi lo ha applicato per programmare la macchina; al computer che guida il dispositivo tecnologico; a chi ha attualizzato il pericolo producendo e mettendo in commercio il veicolo; infine, a chi ha gestito il rischio servendosi della macchina, ovvero cooperando con essa.
A tal proposito, si ritiene opportuno valutare se ai casi specifici si debbano applicare schemi di imputazione della responsabilità declinati sul principio della responsabilità personale e colpevole – come previsto dall'art. 27 Cost. – con finalità rieducativa della pena; oppure se siano preferibili schemi di attribuzione della responsabilità basati sulla causazione oggettiva del danno, incentrati su nozioni quali la "*colpa di programmazione*" o "*di automazione*" che coinvolgano l'impresa produttrice della macchina.

Via Guidubaldo del Monte, 13 - 00197 Roma Tel 06 8417399
razzante@iusconsulting.it www.ranierirazzante.it

È necessario altresì verificare se il problema dell'imputazione possa essere risolto mediante concetti e categorie tradizionali, o se la soluzione debba implicare la creazione di nuove nozioni legali, come l'attribuzione di una "*personalità giuridica artificiale*" alla macchina in tutto o in parte *self-driving*, o quella riferibile ad una forma di cooperazione colposa.
In secondo luogo, si pongono problemi e scelte essenziali di politica del diritto, che il legislatore italiano non ha ancora affrontato.
Dunque, è evidente che vi sia un importante problema di allocazione del rischio, difatti l'attenzione sul tema è altissima, anche in seno alle organizzazioni sovranazionali, primo fra tutti il Consiglio d'Europa.
In riferimento all'attribuzione di responsabilità nel caso di attacco informatico o di reato informatico, occorre chiedersi se le tradizionali categorie del diritto siano applicabili al *web*. La prima ambiguità che si pone è la plausibilità o meno del ritenere che il *web* possa rappresentare un vero e proprio *locus commissi delicti*, ed è ormai pacifico che una realtà diversa da quella fattuale sia idonea alla commissione di reati. Inoltre, le condotte realizzate sul web si estrinsecano nell'emanazione o nella captazione di una serie di impulsi elettronici, interconnessi tra loro, indifferentemente dalla concreta ubicazione del soggetto agente. Per questa ragione il reato assume una connaturata ed inevitabile dimensione transnazionale. Tuttavia, c'è una connessione tra la realtà "reale" e quella "virtuale"; difatti, per accedervi sono necessari appositi strumenti, valute non tradizionali e connessioni idonee a supportare l'esperienza immersiva. Alla luce di queste considerazioni è opportuno interrogarsi, altresì, sulla possibilità concreta che un'azione estrinsecata nel *web*, laddove lesiva di un bene giuridicamente protetto mediante norme penalistiche, possa dar vita a responsabilità. Il Legislatore ha contezza dei rischi derivanti dal mancato riconoscimento di una responsabilità personale per le ipotesi in cui si dovrebbe accettare una *fictio iuris*, come avvenuto per le società e per l'adozione del D. Lgs. 8 giugno 2001, n. 231. In ragione della similarità delle due situazioni, ben potrebbero essere superati i timori in merito al rispetto del principio di personalità della pena rispetto al fatto di reato: sarebbe opportuno porsi a metà strada tra la rilevanza di condotte *contra legem* poste nel Metaverso (così come nel *web*) e, al contrario, una loro assoluta irrilevanza.

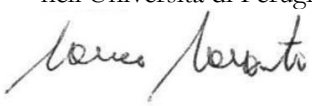
Benché sarebbe utile un riordino della normativa attualmente in vigore, non si ritiene di dover sostenere uno stravolgimento delle fattispecie previste nel Codice penale. Resta, tuttavia, il problema dell'**attribuzione**, non ancora risolto a livello europeo o nazionale. In questo senso, come anticipato, si tratta di spostarsi sul piano interpretativo, poiché è rimessa al Giudice l'attribuzione concreta del reato all'autore. È imprescindibile una considerazione in merito al legame di interdipendenza che intercorre tra il diritto alla prova e l'effettività della tutela penale. Nell'ambito dei reati informatici, infatti, pur disponendo di un *corpus* sanzionatorio esaustivo, questo dovrà necessariamente essere sorretto dall'impiego di conoscenze tecniche specializzate. Pertanto, occorre ampliare il ruolo rivestito dai consulenti tecnici. Non sarebbe inopportuno, allora, ipotizzare **la presenza di un consulente stabile presso le aule giudiziarie**, che coadiuvi le parti ed il giudice. In questo senso, potrebbe pensarsi anche ad un albo professionale apposito: ancora una volta la realtà ed il mondo propongono sfide che il diritto deve riuscire ad accogliere ed affrontare.

Da ultimo, profili problematici connessi alla *cybersicurezza* e all'IA si possono scorgere nello strumento processuale – penale delle **intercettazioni,** che rappresentano - come noto - mezzi di ricerca della prova, con la caratteristica specifica di essere funzionali all'acquisizione di tracce, notizie o dichiarazioni idonee ad assumere rilevanza probatoria e la cui disciplina "*ordinaria*" ha sede negli artt. 266 e ss. c.p.p. Nonostante le novità della c.d. Riforma Cartabia, si coglie l'occasione per porre all'attenzione legislativa alcuni nodi irrisolti. Come noto, attraverso il mezzo di ricerca della prova, fa ingresso nel procedimento penale un elemento probatorio che preesiste allo svolgersi del mezzo stesso. Pertanto, è plausibile che, per il tramite dell'AI, possa essere alterato tale elemento probatorio. In particolare, astrattamente, si potrebbe sia alterare il mezzo probatorio, sia sfruttare le nuove tecnologie per "*confezionare*" prove false o modificate. In tale scenario, si ritiene sia necessaria una dovuta riflessione sulla valenza e sull'affidabilità di tali mezzi di prova, soprattutto qualora l'indagine e il processo si basi prettamente ed esclusivamente su queste ultime per ricercare elementi probatori utili ai fini della configurabilità di una responsabilità penale.

Grazie per l'occasione.

Roma, 8 aprile 2024

In fede
Prof. Avv. Ranieri Razzante
Direttore del Centro di Ricerca
su Sicurezza e Terrorismo
Docente di "Tecniche e regole della Cybersecurity"
nell'Università di Napoli Suor Orsola Benincasa
Docente di "Cybercrime e homeland security"
nell'Università di Perugia



Via Guidubaldo del Monte, 13 - 00197 Roma Tel 06 8417399
razzante@iusconsulting.it www.ranierirazzante.it