FONDAZIONE OCCORSIO

Atti del workshop

INTELLIGENZA ARTIFICIALE E GIURISDIZIONE PENALE

Universitas Mercatorum
Roma, Piazza Mattei, 10
19 novembre 2021

FONDAZIONE VITTORIO OCCORSIO

INDICE

Ragioni di un incontro 3
di GIOVANNI SALVI

Ragioni di una presenza
Interventi di:
LUCIANO CARTA 9
LUIGI GUBITOSI 12
STEFANO LUCCHINI 15
ALESSANDRO PANSA 17

La regolamentazione europea sulla Mutual Legal Assistance (MLA) nel cyberspace 22
di BEATRICE FRAGASSO

Discussione a tre voci 29
Interventi di:
ROBERTO BALDONI
LAURA CARPINI
MASSIMILIANO SIGNORETTI

I.A. e reati ambientali 42
di PASQUALE FIMIANI e GIUSEPPE SGORBATI

I.A. nei reati economici e finanziari 58
di GAETANO RUTA

Criptovalute, aspetti investigativi e processuali 76
di FABIO DI VIZIO

I.A., politica e reati contro la personalità dello Stato 105
di CLAUDIO ORAZIO ONORATI

I.A. e reati "comuni" 129
di MARIO PALAZZI

RAGIONI DI UN INCONTRO

di Giovanni Salvi
Procuratore Generale Corte di Cassazione e
Presidente del Comitato Scientifico FVO

SOMMARIO: 1. Il progetto. – 2. La giurisdizione. – 3. Le monete virtuali, l'*asset recovery*, l'antiriciclaggio. – 4. Le altre prospettive di impiego della I.A. – 5. Le ragioni di un incontro.

1. Il progetto.

La Fondazione Vittorio Occorsio ha, tra i suoi scopi, quello di diffondere tra coloro che operano nel campo del Diritto penale la consapevolezza della necessità di adeguare il metodo dell'investigazione e della prova al suo oggetto.

L'impiego della Intelligenza Artificiale nella commissione di alcuni reati è una sfida davvero significativa. La velocità di trattazione di una enorme massa di informazioni, secondo logiche di apprendimento e di elaborazione che mutano a seconda del tempo e dell'oggetto ma che non necessariamente rispondono a logiche causali, può determinare la trasformazione della struttura del reato ed influire sull'elemento soggettivo dello stesso. Inoltre, si prospettano condotte lesive di interessi di rango costituzionale, che meritano protezione anche penale, ma che appaiono di difficile sussunzione in ipotesi attualmente tipizzate.

L'I.A., peraltro, costituisce uno strumento di prevenzione e potrebbe rivelarsi strumento di indagine rispetto al genere di condotte innanzi descritte; un campo particolarmente significativo è costituito dai crimini ambientali transnazionali.

La transnazionalità è caratteristica connaturata alla I.A.

È bene chiarire, ancora una volta, che il progetto della Fondazione non riguarda i molti impieghi della I.A. nel processo, dalla giustizia predittiva al *profiling*, o nell'organizzazione dell'attività giudiziaria. In questo ambito si inserisce anche il tema della prova scientifica, applicato all'I.A., per le molte questioni che si pongono sull'accesso delle parti alla effettiva logica di funzionamento, ai fini del controllo sia della legittimità della stessa nel processo, sia della attendibilità del risultato. Si tratta di temi di grande importanza ma su di essi vi è ormai ampia consapevolezza e vi sono molte iniziative di ricerca e di applicazione.

È meno esplorato, invece, il campo degli effetti dell'impiego della I.A. sulla struttura del reato e sulla possibilità di effettiva punizione di condotte illecite, per difficoltà probatorie ma soprattutto per il non sempre facile rispetto del principio di legalità e dei suoi corollari.

Si tratta dunque di una nicchia in un'area davvero vasta e nella quale operano soggetti pubblici e privati con grandi potenzialità di analisi e grandi risorse, con le quali la Fondazione non potrebbe competere. Essa ha però un vantaggio, per così dire, di

posizione: può porsi al crocevia di molte e diverse prospettive conoscitive. Utilizzando i risultati e le indicazioni provenienti da quei soggetti, può fungere da luogo di incontro tra le agenzie di *enforcement* (dalla polizia giudiziaria alle autorità indipendenti) e l'autorità giudiziaria, impegnando in questo lavoro le energie interdisciplinari dell'accademia.

Per raggiungere questo risultato, è stato costituito il gruppo di lavoro sull'I.A., suddiviso in quattro sotto-gruppi e in un gruppo di coordinamento. La Fondazione ha iniziato a selezionare il materiale di studio e conoscitivo mirato al tema, come sopra circoscritto, e lo ha messo a disposizione dei partecipanti, per mezzo di cartelle condivise.

2. La giurisdizione.

Dai lavori dei gruppi è emersa la questione della giurisdizione.

In estrema sintesi – e cercando di sottolineare quanto è in corso di discussione in diverse sedi internazionali – il carattere necessariamente transnazionale dei cybercrimes potenzialmente più pericolosi pone da tempo la questione della legittimità (e dei conseguenti limiti) di interventi di accertamento, prevenzione e contrasto da parte dello Stato nazionale di condotte che ledono interessi rilevanti di detto Stato. La giurisdizione si lega al tema – connesso ma distinto – della legittimità (e dei limiti) dell'*enforcement* della giurisdizione, cioè della sua effettiva attuazione attraverso strumenti anche coercitivi.

Il tema intreccia molti aspetti diversi, da quelli di stretta pertinenza del diritto internazionale a quelli – per ciò che qui interessa – del processo penale.

La rapidità delle comunicazioni, parte essenziale della tipologia di condotte qui discusse, rende davvero obsoleto il sistema della collaborazione internazionale basata sulla preventiva richiesta allo Stato nazionale nel cui territorio si svolga un segnamento della condotta (ad esempio, per la presenza di strutture materiali utilizzate dall'agente umano) che si completa o ha riflessi nello Stato rogante, cui segue l'attesa della esecuzione.

La Convenzione di Budapest si è dunque mossa nella direzione di semplificare le procedure di cooperazione, in qualche caso ribaltandone le modalità sulla base del consenso anticipato.

In questi giorni è stato aperto alla firma il Secondo Protocollo Addizionale della Convenzione di Budapest, promossa dal Consiglio d'Europa. Il Protocollo è volto essenzialmente al miglioramento della cooperazione internazionale tra i Paesi aderenti, sulla base della Mutua Assistenza Legale (MLA). Il Protocollo, dunque, affronta i temi emersi nella concreta attuazione della Convenzione, per la diversità di previsioni legali negli Stati Parte, sia per ciò che concerne i casi e le condizioni per l'emissione degli ordini di accesso ai *providers*, sia per le "interferenze" derivanti dal diverso regime della privacy tra UE e altri Paesi, tra cui gli USA. L'approccio della Convenzione e del Protocollo è dunque innanzitutto mirato al tema dell'acquisizione dei dati esterni e di quelli di traffico, nonché di contenuti, custoditi dai *providers*, in un ambiente non localizzato.

Il livello di tale prospettiva è limitato ai problemi conseguenti al *cloud computing* e dunque derivanti dalla localizzazione dell'immagazzinamento dei dati (storage) in luoghi diversi e non sempre noti, nonché dal rapido trasferimento dei dati stessi, a discrezione del *provider*.

Il Protocollo affronta poi il tema della *Volontary Disclosure* da parte dei *providers* come forma principale di esecuzione della MLA.

Il *cloud computing*, tuttavia, non è la frontiera, ma solo uno dei sistemi di immagazzinamento e trattamento del dato. Per l'accertamento e la prevenzione dei reati è, invece, molto più impegnativa la prospettiva che viene dalla estrema rapidità delle operazioni e dalla loro anonimità e non-localizzazione quando le stesse operazioni vengono compiute utilizzando l'I.A., le capacità di calcolo e trasmissione enormemente sviluppati e, in un domani ormai attuale, il *quantum computing*.

La MLA consistente nell'accesso al dato esterno o al contenuto della comunicazione sarà rilevante per i casi meno significativi dei cybercrimes e al contempo del tutto fuori tempo, visti i passaggi che – anche nella più avanzata delle applicazioni della Convenzione e del Protocollo – richiederà giorni, mentre attualmente i tempi di risposta medi sono nell'ordine di molti mesi.

Si riproduce il paradossale effetto per cui la giurisdizione, cioè l'affermazione del potere tradizionalmente caratterizzante la sovranità degli Stati, deve bussare alla porta dell'operatore privato che gestisce come cosa propria un bene pubblico, in questo caso lo Spazio.

Di questa limitazione è ben consapevole anche il lavoro preparatorio per il Protocollo, che considera però non attuale la possibilità di avviare un adeguamento della Convenzione a queste problematiche, limitandosi a segnalarle (a volte solo implicitamente) e a sottolineare che la piena attuazione della Convenzione almeno per i profili attinenti alla MLA nel settore del *cloud computing* è condizione di ogni passaggio successivo.

Emerge dunque la questione della giurisdizione.

L'estrema rapidità delle operazioni che possono essere condotte utilizzando l'I.A. rende inefficace lo strumento della cooperazione. Sembra quasi che l'unica reazione efficace dello Stato "attaccato" sia l'esercizio diretto e immediato dei poteri reattivi, una sorta di affermazione di giurisdizione universale, basata sul principio di territorialità della condotta (di suoi segmenti) o dei suoi effetti.

Naturalmente ciò appare difficilmente compatibile con i principi del diritto internazionale e fonte di continui conflitti per l'affermazione di giurisdizioni concorrenti e con pretese di esclusività.

D'altra parte, non soccorre la disciplina dell'Alto Mare. Solo apparentemente, infatti, il principio di libera navigazione e dei limiti che a tale principio sono posti dal rispetto di interessi nazionali ha diretta analogia con il *cyberspace*. Quest'ultimo, infatti, non ha le nette delimitazioni di spazi territoriali che sono indispensabili per l'attuazione dei principi delle Convenzioni sull'Alto Mare. Ciò non tanto perché le comunicazioni attraversano spazi territoriali, ma perché esse si basano sulla coesistenza di strutture materiali anche in territori diversi, essenziali per il loro funzionamento. Vi è un legame

inestricabile tra territorialità diverse e spazi non territoriali. Ciò rende la situazione nemmeno paragonabile allo Spazio e alla sua disciplina convenzionale.

L'elaborazione del nostro Paese sull'esercizio della giurisdizione in alto mare, che tanto interesse ha destato anche nelle NU, basata sull'interpretazione coordinata delle Convenzioni UNCLOS, di Ginevra, Montego Bay e Londra, sulla Convenzione di Palermo (definizione di crimine transnazionale e protocolli aggiuntivi), nonché sul principio di territorialità, non è dunque applicabile come prospettiva negoziale.

Manipolazioni del mercato che impiegano la rapidissima potenzialità della I.A., che rende anche di difficile individuazione l'effettiva provenienza dell'azione, saranno dunque prive di possibilità di accertamento e di sanzione in sede penale?

La manipolazione del sistema politico di un Paese sotto attacco nell'imminenza delle elezioni sarà contrastata solo dalla successiva ricerca di collaborazione dai molti Stati che avranno registrato sul loro territorio segmenti della condotta?

3. Le monete virtuali, l'*asset recovery*, l'antiriciclaggio.

Di immediato rilievo è poi il tema delle monete virtuali e tra queste delle criptovalute, che qui esaminiamo sotto il limitato profilo dell'asset recovery e dell'antiriciclaggio. Tema che si impone in termini diversi rispetto al passato, per le prospettive di istituzionalizzazione di criptovalute anche nazionali.

L'esame di questi aspetti è urgente, perché di immediato riflesso per la "nicchia" del nostro intervento.

Per l'asset recovery, basti pensare alle recenti questioni postesi per l'utilizzo di criptovalute ai fini societari.

Per il riciclaggio, i problemi sono ovvi e derivano dal meccanismo stesso della criptovaluta, per la riemersione della identificabilità solo al momento della uscita dal circuito cripto. Di immediato rilievo sarebbe dunque la possibilità di operare su ogni tassello della *blockchain*, per aprirne e conoscerne il contenuto transattivo, il che implica l'intromissione in giurisdizioni diverse e non sempre conoscibili in anticipo.

4. Le altre prospettive di impiego della I.A.

Infine, una particolare attenzione va dedicata alla prospettiva di impiego della I.A. nella repressione dei reati di pedopornografia, sulla quale molto avanzato è l'impegno della Polizia Postale.

Sul piano della prevenzione dei reati, un grande spazio sembra oggi emergere nel tema dei reati ambientali, anche per la previsione della centralità del monitoraggio con sistemi complessi dei fatti di inquinamento, che condividono sia grandi banche dati strutturate, che le fonti aperte e infine gli ormai molti e diffusi sistemi di acquisizione di informazione, dai satelliti al monitoraggio climatico, al controllo della movimentazione delle merci ecc.

Sembra quasi che lo spazio della giurisdizione e dunque della risoluzione delle controversie attraverso l'applicazione di regole condivise sia al tramonto. Ma quale potrà essere l'alternativa?

Sul *cyberspace* e sui suoi riflessi sulla regolamentazione delle reazioni dello Stato si discute in diverse sedi internazionali; tra queste sicuramente vi sarà la Prima sessione della Commissione ad hoc istituita dalle Nazioni Unite e nella quale UNODC svolge le funzioni di coordinamento, finalizzata al contrasto dell'utilizzo di sistemi di informazione e comunicazione a scopi criminali che si aprirà il prossimo anno.

Non ci si può nascondere che le prospettive non sono rosee. Si fronteggiano concezioni diverse del *cyberspace*, che corrispondono non solo a visioni diverse della questione ma che in realtà si radicano in contesti istituzionali profondamente diversi.

Se le forti democrazie occidentali, sebbene con visioni tra loro non coincidenti, prospettano uno spazio libero e basato sulla regolazione quasi-volontaria (salvo quando sono in gioco interessi quali la concorrenza ...), i Paesi che si connotano per aspetti autoritari puntano invece sull'affermazione della sovranità statale nella regolamentazione dello spazio virtuale. Se i secondi pongono una grave minaccia alla tutela dei diritti umani, i primi appaiono incapaci di garantire l'effettività dei diritti dei cittadini, se non attraverso meccanismi indiretti, quale la *privacy*.

Lo spazio della giurisdizione penale si perde.

Per accedere ai dati, anche più modesti, occorre bussare alla porta delle Nuove Compagnie delle Indie, che invece ne dispongono liberamente per i loro interessi economici e ormai anche politici. Ma gli spazi vuoti si riempiono e in genere li riempie il più forte.

Il rischio della scomparsa della giurisdizione penale nell'ambiente cibernetico, almeno per i reati più gravi e che offendono interessi fondamentali della società, è ormai imminente. Lo spazio sarà occupato dalla reazione dei singoli Stati, in forme non palesi e progressivamente più forti. Sarà lo spazio del segreto, mentre quello della giurisdizione è lo spazio pubblico delle garanzie.

Premessa per ragionare di queste prospettive è conoscere lo stato della discussione nelle sedi internazionali e i problemi, anche tecnici, che essa pone. Abbiamo quindi invitato al confronto alcuni tra i maggiori esperti italiani in materia.

La Fondazione, dinanzi alla immensità di questi temi, è ben piccola cosa. Essa è una barca a vela in un oceano solcato da corazzate. Ha però un piccolo vantaggio di posizione. Può occupare uno spazio meno noto, al crocevia tra competenze disciplinari diverse, che è costituito dalla esperienza nella trattazione degli aspetti sostanziali e processuali dei reati.

Ciascuno di questi aspetti è oggetto di studio nell'ambito dei gruppi di lavoro della Fondazione. Occorre oggi che su di essi si concentri l'attenzione coordinata dei diversi gruppi.

Il contributo della nostra specificità potrà venire dall'esame di *study cases*, di vicende recenti individuate come significative e che saranno esaminate dal punto di vista della giurisdizione applicata alle condotte, quali accertate.

Ogni gruppo dovrà quindi individuare uno o più casi, che costituiranno oggetto di indagine nel gruppo, poi condivisa in seminari aperti.

5. Le ragioni di un incontro.

Sono queste le ragioni dell'incontro tra i coordinatori dei gruppi di lavoro, aperto ai principali soggetti privati e istituzionali che collaborano con la Fondazione su questo tema, per l'organizzazione del nostro impegno nei prossimi mesi e in vista del contributo che intendiamo dare alla diffusione tra gli operatori del Law Enforcement e della partecipazione alla Conferenza delle Nazioni Unite sul Crimine Transnazionale del prossimo anno.

RAGIONI DI UNA PRESENZA

Intervento di Luciano Carta, Presidente di Leonardo.

Chi come noi è nato nel Secolo breve ha subìto il fascino dell'intelligenza artificiale. Col tempo il mito della delega alle macchine è stato catturato dalla complessità del mondo: un importante momento di snodo lo abbiamo vissuto con il contemporaneo sviluppo della tecnologia digitale e della globalizzazione, da un lato, e la diffusione del neoliberismo, dall'altro. Il digitale – in tanti settori, incluso quello dell'informazione – ha disintermediato il rapporto tra cittadini e Stato. Lo stesso è accaduto nel settore della giustizia, dove la *legaltech* ha per certi versi disintermediato il rapporto tra cittadini e professionisti del diritto. Aprendo così la strada al tema della prevedibilità giuridica e contribuendo ad alimentare il mito di un mondo in cui i rapporti sociali siano modellabili dall'innovazione tecnologica, sottratti al rischio di soggettivismo e di arbitrio da parte dell'uomo.

È apprezzabile il fatto che l'importante progetto della Fondazione Vittorio Occorsio di cui oggi condividiamo i primi risultati non riguardi tanto la giustizia predittiva o gli altri usi dell'Intelligenza Artificiale nel processo penale, bensì il meno esplorato campo degli effetti dell'impiego dell'Intelligenza Artificiale sulla struttura del reato e sulla possibilità di effettiva punizione di condotte illecite (dal campo economico –finanziario al riciclaggio e alle frodi informatiche fino al traffico di stupefacenti tramite l'utilizzo di droni, tanto per fare qualche esempio).

Il punto è proprio questo: ora che sappiamo che una macchina "intelligente", in grado di auto-apprendere e di agire autonomamente, può in astratto anche causare danni e infrangere la legge, essa ci appare meno fascinosa.

Senza cedere alla tentazione di alimentare nuovi miti o distruggerne vecchi, ma tenendo in debito conto i rischi per la sicurezza e la tutela dei diritti fondamentali che Parlamento e Commissione europea ci hanno recentemente indicato come inaggirabili, quando trattiamo di Intelligenza Artificiale dobbiamo restare con i piedi per terra. E partire da un elemento incontrovertibile: i dati sono la spina dorsale delle nuove tecnologie. Le tecnologie che consentono alle macchine di prendere decisioni in forma autonoma – *"Machine learning"* e *"Deep learnig"* – si basano nel primo caso su dati strutturati, un addestratore umano, un database controllabile, e un algoritmo variabile, mentre nel secondo caso su dati non strutturati, un sistema di autoapprendimento, un insieme di basi di dati molto vasto e una rete neurale di algoritmi. Sono sistemi molto potenti con margine di maturazione abbastanza ampi. Un fatto è però certo: se al sistema viene fornita sin dall'inizio una base di dati in entrata errata, la scelta e le decisioni conseguenti all'elaborazione di tali dati non potrà che essere sbagliata. "*Garbage in, garbage out*": se immetti spazzatura, alla fine del processo non avrai altro che spazzatura, l'efficace sintesi di taluni. Come può esser utile questo warning all'importante lavoro della Fondazione Occorsio? Innanzitutto, a mio parere, nell'interrogarci sull'omogeneità e sull'aggiornamento delle banche dati alla base della nostra analisi: quelle che rilevano

la tipologia di reato, la frequenza, l'ambito e così via. Le fonti possono essere le più diverse: forze dell'ordine, tribunali, *databrokers* ma anche social network o internet. Se puntiamo a un modello attendibile, il processo di analisi sugli effetti dell'impiego dell'Intelligenza Artificiale sulla struttura del reato deve partire da una scelta e da una messa a fattor comune delle banche dati da cui si intende partire.

Qualora infatti i dati forniti al sistema siano viziati da pregiudizio, l'*outcome* dell'algoritmo rifletterà o amplificherà il medesimo pregiudizio. Gli algoritmi di *predictive policing*, ad esempio, diffusamente impiegati negli Stati Uniti, cominciano a prendere piede anche in alcune questure italiane (Napoli e Milano), con lo scopo di individuare luoghi sospetti o elaborare profili criminali individuali di persone a rischio. Simili sistemi predittivi applicati in campo processuale non sono consentiti in ambito Ue, contrariamente a quanto accade negli Stati Uniti dove una non corretta immissione di dati sulla pericolosità di soggetti correlata alla loro origine etnica ha determinato l'errata attribuzione di un rischio di recidiva maggiore (caso Loomis-Compas del 2017[1]).

L'attendibilità e l'integrità del dato, dunque, sono ciò che va garantito in primis, assieme alla messa in sicurezza del sistema su cui "gira" il sistema di Intelligenza artificiale. Siamo immersi nel digitale, che costituisce la nuova dimensione del mondo in cui viviamo. Le tecnologie digitali sono alla base del funzionamento di infrastrutture che erogano servizi essenziali per i cittadini come, ad esempio, energia, trasporti, sanità, banche, telecomunicazioni. Proteggere l'innovazione è oramai una priorità. Lo spazio *cyber* e quello extra-atmosferico, anche per la loro natura duale – civile e militare – sono le nuove dimensioni della conflittualità. Le applicazioni dell'intelligenza artificiale, così come tutti i fenomeni digitali, non si fermano davanti alle frontiere. Ciò vale anche nei casi di violazione: gli hacker fanno amicizia in fretta, mentre i Governi necessitano di tempi biblici per collaborare e accordarsi a livello internazionale. Sull'urgenza di una corretta regolamentazione dell'Intelligenza Artificiale negli ultimi mesi hanno fatto sentire la loro voce non solo l'Unione europea e il Consiglio d'Europa: il dibattito sembrerebbe a un'imminente svolta anche negli Stati Uniti dove i consiglieri scientifici del presidente Biden sono al lavoro su una "Carta dei diritti". Tracciare il confine tra il lecito e l'illecito significa avere ben presente il principio di supremazia della legge, o meglio il rischio che tale principio possa esser minato da un uso senza regole dell'Intelligenza artificiale. Una consapevolezza, questa, accompagnata da interrogativi etici, filosofico-normativi e considerazioni geopolitiche nel rapporto dell'uomo con la macchina.

Passi avanti si stanno facendo anche in Italia, per quanto riguarda la tutela del cyberspazio. L'Agenzia nazionale per la cybersicurezza, guidata dal prof. Baldoni, può contare su una squadra di esperti capaci di realizzare importanti sinergie tra l'industria, la ricerca, le forze di polizia e il mondo dell'intelligence. Garantire la sovranità nazionale del dato è di fondamentale importanza**.** Per questo l'azienda che mi onoro di presiedere, Leonardo, ha presentato assieme a Cassa Depositi e Prestiti, Sogei e Tim una proposta di partenariato pubblico-privato per la creazione del Polo Strategico Nazionale,

[1] *Loomis v. Wisconsin*, 881 N.W.2d 749 (Wis. 2016), cert. denied, 137 S.Ct. 2290 (2017).

un'infrastruttura per la gestione in *cloud* di dati e applicazioni della Pubblica Amministrazione.

In definitiva, dobbiamo puntare sulle opportunità di sviluppo tecnologico orientato allo sviluppo di algoritmi di Intelligenza Artificiale consolidati. Perché nessuno di noi, uomini e donne del Secolo breve che hanno subito la fascinazione di un robot o di una macchina super intelligente, vorrebbe che la storia finisse come nell'ultimo romanzo di Ian McEwan, "Macchine come me"[2]: il protagonista, Charlie, uccide il robot antropomorfo, Adam, acquistato con i soldi dell'eredità materna. Lo uccide perché il robot sta per denunciare la sua compagna, Miranda, per essersi vendicata in passato di un uomo violento accusandolo falsamente di un grave reato. La pura (e programmata) tensione alla giustizia dell'androide si scontra con la fragilità dell'umano sentimento vendicativo. I confini vanno ben tracciati: macchine sì, ma non come noi; uomini sì, ma non come macchine.

[2] I. McEwan, *Macchine come me*, Einaudi, 2019.

Intervento di Luigi Gubitosi, già Amministratore Delegato e Direttore Generale TIM

SOMMARIO: 1. I.A. e le attività di *law enforcement* (polizia predittiva). – 2. I.A. e decisione giudiziaria ("*automated decision systems*"). – 3. I.A. e valutazione della pericolosità criminale ("algoritmi predittivi"). – 4. I.A. e commissione di un reato.

La convenzione del Consiglio d'Europa sul *Cybercrime* – siglata a Budapest nel 2011 e aggiornata di recente con un nuovo protocollo – dispone chiaramente un obbligo di cooperazione tra le autorità giudiziarie dei vari Paesi in materia di *cybercrime*.

Le autorità giudiziarie dei singoli Stati devono dunque supportarsi a vicenda in caso di ordini di estradizione o di richieste di informazioni, coinvolgendo ovviamente i soggetti pubblici e privati che detengono quelle informazioni.

Dalla Convenzione di Budapest emerge l'urgenza di svolgere attività omogenee e molto estese, inclusa la conservazione dei dati per periodi particolarmente lunghi. In quest'ottica, TIM si è messa a disposizione delle autorità italiane e internazionali, al fine di rendere efficaci i principi della Convenzione.

Nello specifico, mi sembra che gli scenari che implicano l'utilizzo dell'I.A. e che sollevano questioni di diritto penale siano quattro:

1. le attività di *law enforcement* e, in particolare, le attività di polizia predittiva;
2. i c.d. *automated decision systems*, che potrebbero essere impiegati anche all'interno dei procedimenti penali, sostituendo in tutto o in parte la decisione del giudice;
3. i c.d. algoritmi predittivi, impiegati per valutare la pericolosità criminale di un soggetto, cioè la probabilità che costui commetta nuovamente un reato;
4. le possibili ipotesi di coinvolgimento di un sistema di I.A. nella commissione di un reato.

1. I.A. e le attività di *law enforcement* (polizia predittiva).

Si tratta dei possibili impieghi dei sistemi di I.A. nelle attività di *law enforcement* rivolte alla prevenzione dei reati. Fermo restando che è indubbio che i sistemi di polizia predittiva possono essere di grande utilità nella prevenzione, il loro utilizzo, al momento, suscita non poche perplessità, per i seguenti motivi:

(i) non è stato regolato a livello normativo in nessun Paese, sicché le modalità di utilizzo e la valutazione dei loro risultati finiscono per essere affidate alla sensibilità e all'esperienza degli operatori di polizia;

(ii) potrebbe implicare gravi incompatibilità con la normativa sull *privacy* (data l'elevata mole di dati personali raccolti), e con il divieto di discriminazione (nei casi in cui si identifichino fattori di pericolosità connessi a caratteristiche etniche, religiose o sociali);

(iii) sollecita una prevenzione dei reati attraverso l'intervento della polizia, senza mirare alla riduzione del crimine attraverso azioni "a monte", rivolte cioè ai fattori originari del reato (fattori sociali, ambientali, individuali, economici, etc.).

2. I.A. e decisione giudiziaria ("*automated decision systems*").

Anche a fini decisionali, in vari ambiti vengono già da tempo utilizzati diversi algoritmi basati sull'I.A. Si tratta dei cosiddetti *automated decision systems*.

Tra le decisioni che questi algoritmi possono assumere rientrano soprattutto quelle finalizzate a comporre – o a prevenire – controversie, che ad oggi riguardano prevalentemente questioni civilistiche (risarcimento danni, gestione di pratiche assicurative, danni da prodotto, etc). Nulla esclude, tuttavia, che a breve gli algoritmi decisionali possano trovare impiego anche in ambito penale.

L'impiego di algoritmi decisionali nel nostro ordinamento giuridico potrebbe tuttavia risultare critico per almeno tre motivi:

(i) il mezzo di prova più frequentemente utilizzato nel processo penale è la testimonianza, ed un computer incontrerebbe difficoltà nel giudicare se un teste abbia detto la verità, sia stato reticente o abbia mentito;

(ii) plurimi e non predeterminati sono i criteri di valutazione della prova, per cui – specialmente in un processo indiziario – sarebbe difficile per un algoritmo stabilire se determinati indizi possano essere considerati "gravi, precisi e concordanti" (art. 192, comma 2, c.p.p.);

(iii) pare difficile che un algoritmo possa comprendere e applicare la regola di giudizio basata sull' "oltre ogni ragionevole dubbio" (art. 533, comma 1, c.p.p.): possiamo immaginare *software* capaci di dare risposte con logica binaria (sì/no; bianco/nero; vero/falso), o probabilistica (sì al 70%; bianco all'80%; vero al 90%), ma difficilmente *software* capaci, almeno ad oggi, di esprimere valutazioni basate su fattori "umani".

3. I.A. e valutazione della pericolosità criminale ("algoritmi predittivi").

Gli algoritmi predittivi hanno l'obiettivo di valutare la probabilità che un individuo, con determinate caratteristiche, possa commettere un reato – aspetto necessario quando si tratta di applicare misure di sicurezza, cautelari o di prevenzione, o anche per concedere la sospensione condizionale di una pena.

Già da una decina d'anni negli USA sono diffusi algoritmi predittivi della pericolosità criminale. L'esperienza è, per molti versi, positiva, ma ha anche rilevato dei *bias*: la pericolosità predittiva, ad esempio è nella maggioranza dei casi attribuita sulla base di specifiche caratteristiche etniche.

Ad oggi, almeno in Europa, gli algoritmi predittivi della pericolosità criminale non hanno avuto accesso nelle aule penali, grazie all'art. 22 GDPR, in base al quale «[l]'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente

sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona».

4. I.A. e commissione di un reato.

Quanto alle possibili ipotesi di coinvolgimento di un sistema di I.A. nella commissione di un reato, due sono gli aspetti principali da prendere in considerazione: da un lato, l'utilizzo di sistemi di I.A. come "strumenti" di commissione del reato, dall'altro la possibile realizzazione di un reato che vede il sistema di I.A. quale "autore" o "vittima" del reato.

(i) Utilizzo di sistemi di I.A. come "strumenti" di commissione del reato.

Le enormi potenzialità dell'I.A. potrebbero essere asservite anche a scopi criminali. Un esempio, sul piano finanziario, è costituito dalle potenziali condotte di manipolazione abusiva del mercato, che possono essere commesse attraverso *software* a cui è affidata non solo l'esecuzione delle transazioni finanziarie, ma anche la stessa decisione di compierle, sulla scorta di un algoritmo che compara numerose variabili.

(ii) Sistema di I.A. quale "autore" e "vittima" del reato.

Tale aspetto riguarda i casi in cui il sistema di I.A. sia fornito di capacità di autoapprendimento e di autonomia decisionale. Quando la condotta dell'uomo si interseca con l'attività di un sistema di I.A., il percorso di attribuzione delle responsabilità si complica, in quanto il fatto illecito non è più opera esclusiva dell'uomo.

Il presupposto per imputare al programmatore (o all'utente) la responsabilità per danni generati dall'I.A. coincide con il controllo che tale individuo è in grado di esercitare sul *software*; controllo che verrebbe meno nei casi in cui è stata sviluppata la capacità di autoapprendimento della macchina.

Alcuni degli argomenti che potrebbero indurre a considerare il sistema di I.A. quale "persona" potrebbero fornire elementi anche a favore di un suo riconoscimento come possibile vittima del reato. Osta a tale riconoscimento, tuttavia, l'idea che i sistemi di I.A. non hanno veri sentimenti. Ciò non esclude, in ogni caso, che possa essere opportuna l'introduzione di nuove figure di reato che rendano punibili gli attacchi rivolti ai sistemi di I.A., che ad oggi non sembrano trovare adeguata tutela penale nelle vigenti disposizioni.

Intervento di Stefano Lucchini, Chief Institutional Affairs and External Communication Officer Intesa San Paolo.

Buongiorno, saluto innanzitutto con grande stima e affetto il Presidente Salvi, la Professoressa Decaro, il Prof. Vittorio Occorsio e gli amici della Fondazione. Purtroppo, impegni concomitanti non mi hanno permesso di partecipare a questo incontro in presenza.

Mi fa particolarmente piacere partecipare oggi a questo primo *workshop* su "Intelligenza artificiale e giurisdizione penale" per almeno due ordini di ragioni. Innanzitutto, sostengo convintamente – sia a livello personale, che in qualità di rappresentante di Intesa San Paolo –il fondamentale lavoro di testimonianza e ricerca svolto da questa prestigiosa Fondazione. In secondo luogo, ritengo che ogni approfondimento sul vasto tema dell'Intelligenza Artificiale sia indifferibile, anche per offrire alle Istituzioni il necessario supporto affinché possano regolarne in modo ottimale sviluppo e implicazioni esplicite ed implicite.

Se ci confrontiamo sulle ragioni di una presenza, consentitemi di fare una breve digressione che può forse aiutarci ad inquadrare la portata anche filosofica della rivoluzione indotta dall'Intelligenza Artificiale.

Conversando recentemente con Luciano Violante, un amico e grande giurista, ho appreso come non sia corretto rapportarsi all'I.A. come a un fenomeno estraneo e terzo rispetto a noi, cittadini, professionisti o imprese.

L'I.A. – nella misura in cui è ormai realtà di ogni giorno, è pervasiva, è ovunque – diviene ambiente in cui viviamo e muoviamo. Questo cambio di prospettiva rende urgente e necessario il confronto sulle opportunità e i problemi posti dalle sue applicazioni.

Se questo è vero nella società in cui viviamo o nel quadro delle attività economiche e finanziarie, perché non dovrebbe esserlo nell'ampio quadro della (tentata) regolamentazione del *cyberspace*?

È probabilmente dalla condivisione di questa interpretazione che il Gruppo Intesa Sanpaolo, nell'accostarsi all'ambiente dell'I.A., ha da tempo adottato un approccio che potremmo definire olistico.

Per questo motivo, abbiamo recentemente sposato, ad esempio, l'idea di costituire insieme a Tim un Osservatorio permanente su etica e applicazioni di Intelligenza artificiale nel vasto dominio delle attività economico-commerciali.

Per la stessa ragione, la banca sta definendo il lancio di un *hub* dedicato allo studio e alla sperimentazione di soluzioni di *Artificial Intelligence* utili a rafforzare le procedure interne poste a contrasto dei crimini di natura finanziaria.

In questo contesto, il ricorso all'Intelligenza Artificiale nella lotta al crimine finanziario è cruciale, non solo perché consente l'analisi di enormi masse di informazioni in brevissimo tempo, ma perché si basa essa stessa su contributi multidisciplinari che spaziano dalla *computer science* alla matematica applicata.

Le istituzioni finanziarie "tradizionali" sono da tempo impegnate in un'azione di sistema con le autorità di vigilanza, per massimizzare ed efficientare le soluzioni

innovative di controllo delle cd. operazioni sospette. Queste iniziative hanno poi assunto un'importanza capitale con il rapido diffondersi a livello internazionale di criptovalute e *blockchain* – strumenti che hanno mostrato tutta la loro efficacia in termini di rapidità e crescente sicurezza di esecuzione, senza però mai offrire garanzie sul piano della puntuale identificazione dei soggetti coinvolti e della visibilità dell'oggetto/contenuto della transazione.

Andando poi all'oggetto della nostra analisi riterrei urgente porre l'accento sulla nuova natura del reato commesso attraverso l'impiego di intelligenza artificiale. È innanzitutto corretto parlare di un nuovo tipo di reato o si tratta di reati tradizionali perpetrati tramite il ricorso all'Intelligenza Artificiale?

Se la questione non è del tutto pacifica – e se si vuole andare al di là di categorie generiche come "reato informatico" – si potrebbe dire che con "*A.I.-Crime*" si indicano quei reati realizzati con l'utilizzo di Intelligenza artificiale, intendendo quest'ultima come una macchina che – per utilizzare la definizione classica di John McCarthy del 1955 –utilizzi un proprio linguaggio, formi astrazione e concetti, migliori sé stessa, risolva problemi, si comporti con modalità che sarebbero chiamate "intelligenti" se a porle in essere fosse un umano.

Se questo è il perimetro di gioco, diviene di conseguenza essenziale individuare il responsabile del reato commesso per mezzo dell'Intelligenza Artificiale. Da qui la domanda: l'agente responsabile può essere individuato in una macchina?

In principio *Machina delinquere (non) potest*. Secondo una prima lettura, Luciano Floridi, partendo dalle riflessioni di McCarthy, ritiene che gli Agenti Artificiali – così definiti – siano sufficientemente informati, intelligenti, autonomi per compiere azioni moralmente rilevanti, indipendentemente dagli umani che li hanno creati.

Ad un secondo sguardo, in particolare alle concrete e specifiche applicazioni che vediamo realizzarsi sotto i nostri occhi, appare forse più ragionevole sostenere che la macchina può dirsi intelligente nella misura in cui sì completa un compito e impara in modo interattivo dalla sua stessa esecuzione, ma il suo successo richiede di norma l'intervento umano. Dall'interdipendenza uomo-macchina deriverebbe l'impossibilità di attribuire alla sola macchina la "consapevolezza" e "volontà" dell'agire.

Tale interdipendenza uomo-macchina non pare poi smorzarsi anche nel caso di macchine evolute, che in base a sofisticati meccanismi di autoapprendimento ("*machine learning*") assumono decisioni.

All'insorgere di un reato – anche in conseguenza della decisione "assunta" dalla macchina – appare controverso attribuire alla stessa una *free voluntary action*. Una volontà, insomma, che in ultima analisi parrebbe al momento restare ancorata all'azione dell'agente umano.

In conclusione, permettetemi di offrire due riflessioni di carattere generale.

In primis, l'I.A. è uno strumento molto potente e "neutro", utilizzabile tanto dai criminali quanto dai benefattori: la grande sfida sta nel saperla usare per un nobile fine.

In secundis, la regolamentazione di settore deve, da un lato, rendere l'I.A. sicura e, dall'altro, promuoverne la diffusione e lo sviluppo.

4. Intervento di Alessandro Pansa, Presidente TI SPARKLE.

Ringrazio, innanzitutto, tutti i partecipanti a questo seminario.

In questo mio breve intervento vorrei portare alla vostra attenzione un mio dubbio.

Sono convinto che si riuscirà a risolvere sul piano convenzionale il tema della giurisdizione e anche quello delle forme migliori di cooperazione giudiziaria internazionale. Ci vorrà del tempo, ma confido molto sul fatto che si arriverà al risultato voluto. Sono convinto, allo stesso modo, che con il contributo di esperti di livello come quelli chiamati dalla Fondazione Occorsio saranno trovate le soluzioni normative sia sul piano processuale che sostanziale. Certo, non sarà facile; ma l'intelligenza dei giuristi, coniugata con le capacità diplomatiche, porterà di sicuro a tracciare un perimetro entro il quale il giudice potrà esercitare la giurisdizione.

La domanda che tuttavia mi pongo, a questo punto, è la seguente: saremo in grado, dal punto di vista tecnico, di eseguire le azioni concrete che servono all'acquisizione della prova, sia sul piano investigativo che dibattimentale?

La normativa internazionale, come quella che l'U.E. ha già proposto la primavera scorsa[3], stabilirà ad esempio quali saranno le attività che non potranno essere svolte da alcuni (come l'acquisizione delle informazioni personali da parte delle aziende) ma consentite ad altri (ad esempio, in sede di indagini preliminari).

Prendendo ad esempio il tema 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?

Non possiamo porci solo la questione di quali principi e quali regole disciplineranno la giurisdizione o l'acquisizione della prova. Dobbiamo porci anche una seconda domanda: che cosa siamo o saremo in grado di fare, per dare seguito alle norme che verranno emanate? Avremo la tecnologia che ci consentirà di scoprire i reati che vedono coinvolta l'A.I., di assicurare l'esecuzione corretta delle regole fissate? Avremo la tecnologia adeguata per garantire l'acquisizione della prova?

Il nostro Paese non produce *microchip*, non produce *hardware* complessi. Insomma, nel settore delle tecnologie dipendiamo essenzialmente dall'approvvigionamento estero – un po' come per le fonti energetiche. Questo ci pone tecnicamente su un piano di debolezza.

Va anche aggiunto che accanto alla carenza industriale, vi è anche quella rappresentata dalla circostanza che i grandi operatori del settore, i c.d. *Over-The-Top* (OTT), sono tutti stranieri (principalmente statunitense e cinesi, ma non solo).

Se, ad esempio, l'autore del reato fosse un OTT che risiede all'estero, con quali strumenti ci presenteremo nelle sedi di questa azienda per acquisire la prova (sempre

[3] Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione - 2021/0106 (COD) del 21 aprile 2021.

che, sulla base delle norme ordinarie in tema di giurisdizione, ci sia la concreta possibilità di processare una di queste compagnie in Italia)? 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? Avremo le tecnologie per acquisire la prova forense? E ancora, saremo in grado di accedere (e di comprendere) gli algoritmi che si sono comportati come veri e propri "autori materiali" del reato?

Anche l'autorità giudiziaria dovrà cominciare ad utilizzare sistemi di I.A., al fine di portare avanti in maniera efficace la funzione giurisdizionale?

In poche parole, mi sembra che in futuro dipenderemo molto dalla volontà dell'autore del reato. Da persona che ha svolto le funzioni di "investigatore" per molto tempo, credo che l'unica possibilità di acquisire una prova attendibile sul piano processuale sarà la confessione. Un gigante del WEB o dell'industria tecnologica che confessa… Speriamo bene!

Ricapitolando, in primo luogo, credo che quello che ci servirà sarà una forte capacità negoziale a livello internazionale, che consenta anche ad attori deboli – quali noi siamo e la stessa Unione Europea è – di non soccombere. Confido nel fatto che – anche grazie al ruolo dell'UE – riusciremo a trovare una qualche soluzione normativa. Il percorso, tuttavia, sarà lungo ed accidentato.

In secondo luogo, resta il problema del *gap* tecnologico. Saremo in grado di colmarlo? Quanto tempo avremo per poter implementare strumenti di I.A.? Ricordiamoci che il tempo non è una variabile indifferente, poiché la velocità dello sviluppo tecnologico è notevole e non è programmata: le accelerazioni sono improvvise e spesso impreviste.

Detto questo – senza piangerci addosso – abbiamo una scelta immediata da fare, che potrà dare poi sostegno concreto alla giurisdizione penale: investire al massimo in innovazione, puntando a quei settori che sono oggi agli albori e che solo studio, ricerca e intelligenza umana potranno consentirci di sviluppare. È tutto qui: studio, ricerca e intelligenza umana. Non dobbiamo provare semplicemente a realizzare prodotti concorrenziali a quelli esistenti o in fase di sviluppo, per i quali ci vogliono risorse ingenti e tempi lunghi. Dobbiamo guardare ai traguardi futuri della scienza e mirare soprattutto a quelli. Cosa sarà in grado di fare l'A.I. in un futuro prossimo?

Siamo in una fase di grande ed ulteriore cambiamento rispetto allo stato di sviluppo delle tecnologie esistenti. L'intelligenza artificiale ha agito come il principale motore delle tecnologie emergenti (si pensi a *big data*, robotica e *Internet of Things*) e continuerà ad agire come innovatore tecnologico per il futuro. Insieme alla meccanica quantistica e alle sue applicazioni in materia di comunicazioni e di computer, il nostro futuro è già segnato da queste innovazioni. Il mondo che oggi conosciamo cambierà radicalmente: è questione solo di "quando" e di "come", ma certamente non di "se". Non sembri esagerato quello che dico. Pensate a noi tutti prima e dopo il cellulare. Vi ricordate quando il telefono fisso *cordless*, che ci consentiva di girare per casa parlando a telefono, ci sembrava una cosa eccezionale?

Credo, pertanto, che mentre il mondo della Giustizia si interessa di I.A., quello dell'Istruzione, quello della ricerca, quello dell'innovazione tecnologica e dello sviluppo

economico dovrebbero interessarsi prevalentemente all'*Artificial General intelligence* (A.G.I.), che costituisce il prossimo futuro.

Quando oggi noi parliamo di I.A., infatti, ci riferiamo a quella specializzata, che sa fare alcune cose, che le migliorerà man mano che aumenterà la sua esperienza utilizzando le sue capacità di apprendimento. Questo riguarda però una singola attività; per quanto complessa possa essere, sarà sempre la riproduzione di un'attività specifica dell'uomo (quelle ripetitive, standardizzate, con procedure rigide e rigorose). Se vogliamo svolgere invece un'attività diversa, allora dovremo ricorrere ad un altro sistema di I.A., dotato di un altro *software*. Ognuno di questi sistemi, grazie al *machine learning*, implementerà sempre più le sue capacità, tanto da diventare imbattibile in quella specifica ed unica attività. Il *machine learning* è cosa in parte superata; oggi si parla già di *deep learning* e di *reinforcement learning*, che progrediscono verso modelli cosiddetti neuroevolutivi: alcuni ricercatori dell'MIT sono già stati in grado di incorporare in questi sistemi alcune abilità sociali (c.d. *social skills*), che hanno consentito a due robot di interagire tra loro.

Quando ci riferiamo invece all'*artificial general intelligence*, dobbiamo immaginare un sistema interdisciplinare, in grado di ottimizzare le sue diverse conoscenze e le sue diverse competenze per risolvere problemi di molteplice natura. L'A.G.I. non avrà semplicemente la capacità di riprodurre una singola attività dell'uomo, ma potrà pensare come un essere umano di spiccata intelligenza. In un prossimo futuro potrà essere sviluppato un supercalcolatore quantistico con capacità complesse, in grado di imitare l'insieme dei processi mentali dell'uomo, risolvendo anche schemi conflittuali. A parte i temi etici e le preoccupazioni del rapporto tra uomo e macchina – che trovano spazio in dibattitti diversi da quello odierno – dobbiamo prendere atto che la tecnologia dell'*High Performance Computing*[4] e la tecnologia necessaria per entrare nel mondo quantistico stanno nascendo oggi.

Questa è la prossima frontiera che segnerà una nuova supremazia, quella quantistica. Già abbiamo degli esempi concreti: un processore di Google, *Sycomore*, nel 2019 ha segnato un record di velocità nel completamento di *task* molto complesse, al punto da mettere in ombra le prestazioni di *Summit*, il supercomputer sviluppato da IBM.

Al momento non sono chiari tutti gli aspetti e tutti i limiti di questa nuova avventura dell'uomo, ma quel che è certo è che i computer quantistici sono in grado di decifrare qualsiasi informazione e rompere in millesimi di secondo i codici di crittazione basati su algoritmi classici. Possono così diventare spie incontrollabili, che possono essere fermate solo di fronte ad ulteriori comunicazioni quantistiche, che offrono una protezione più sofisticata e sono considerati "a prova di *hacker*".

Nel momento in cui questi strumenti saranno operativi, la localizzazione dell'origine delle azioni governate dall'intelligenza artificiale sarà molto più difficile da

[4] "Con *High Performance Computing* (HPC) (che può essere tradotto, in italiano, come "calcolo ad elevate prestazioni"), ci si riferisce, in informatica, alle tecnologie utilizzate da computer cluster per creare dei sistemi di elaborazione in grado di fornire delle prestazioni molto elevate nell'ordine dei PetaFLOPS, ricorrendo tipicamente al calcolo parallelo.

individuare di quanto non lo sia già oggi. Sarà molto più difficile scoprire se un reato è stato commesso, se una cosa sia vera o virtuale. Per questo motivo, ribadisco che – a mio avviso – il tema della giurisdizione deve correre di pari passo con quello dell'innovazione tecnologica.

Come ha affermato Max Tegmark, professore di fisica al MIT, in un TED Talk del 2018[5], la maggior parte dei ricercatori esperti in materia si aspetta la realizzazione dell'A.G.I. entro decenni. Ma i tempi potranno anche dimezzarsi. Il trovarsi impreparati davanti all'A.G.I. potrebbe rivelarsi il più grande errore nella storia umana. Nelle parole di Max Tegmark: «Potrebbe consentire una brutale dittatura globale con disuguaglianza, sorveglianza, sofferenza senza precedenti e forse anche l'estinzione della razza umana. Ma se agiamo con attenzione, potremmo finire in un futuro fantastico in cui tutti stanno meglio: i poveri sono più ricchi, i ricchi sono più ricchi, tutti sono sani e liberi di vivere i propri sogni».

Insomma, se non vogliamo restare per sempre dipendenti dalle tecnologie sviluppate all'estero, dovremmo forse cercare di sviluppare una nostra A.G.I. Così, tra l'altro, raccomanda l'Unione europea, che in questo campo ha una postura visionaria, diversamente da molti altri settori in cui è meno aperta. L'Ue, infatti, intende conquistare una posizione primaria a livello mondiale, non commettendo gli stessi errori che sono stati commessi in altri settori del digitale. Di particolare importanza è lo *European Flagship on Quantum Technologies*[6], il programma lanciato ormai tre anni fa dall'Unione Europea, finalizzato a sviluppare una politica di sviluppo delle nuove tecnologie, consapevole che da esse potranno derivare enormi benefici in molti ambiti: si pensi, ad esempio, al settore dei trasporti e delle telecomunicazioni, della difesa, della formazione, dell'ecologia, della salute, della giustizia. L'evoluzione di queste tecnologie potrà condurre alla cosiddetta supremazia quantistica, ovverosia alla complessiva superiorità di coloro che ricorrono a questa tecnologia, rispetto agli altri che non ne dispongono.

L'intelligenza artificiale generale è un traguardo futuro, che in questo momento non siamo in grado di misurare temporalmente. Ma si badi bene, non si tratta di un mero esercizio teorico o di una sfida tra scienziati. Se non partecipiamo alla competizione in questo settore, potremo anche approvare nuove regolamentazioni giuridiche di diritto processuale, ma esse saranno già superate dalle nuove tecnologie. La domanda di giustizia non riguarda solo l'ordinamento giuridico, ma anche la supremazia tecnologia.

In conclusione, il mio auspicio è che si punti sulla ricerca scientifica nel campo dell'A.G.I. e della meccanica quantistica – oltre che sul processo di adeguamento e ammodernamento dell'apparato normativo, a cui questa iniziativa meritoria mira. È indispensabile dedicare, fin da ora, tutte le risorse necessarie all'*High Performance Computing* e alle tecnologie quantistiche in tema di *computing* e di *communication*. Proprio in tal senso, tra l'altro, mi sembra che si esprima il dott. Cappellini, nelle note

[5] Il video è disponibile sul sito di TED, a questo link: https://www.ted.com/speakers/max_tegmark.

[6] *Quantum Technologies Flagship* è un'iniziativa di ricerca e innovazione a lungo termine che mira a mettere l'Europa in prima linea nella seconda rivoluzione quantistica. Il progetto *Quantum Technologies Flagship* dovrebbe sostenere il lavoro di centinaia di ricercatori quantistici in 10 anni, con un budget previsto di 1 miliardo di euro dall'UE.

metodologiche trasmesse, quando afferma che «occorre incrociare sia l'intuito del penalista, più che altro del p.m., o dell'investigatore, con la conoscenza del tecnico: la prima, ad esempio, per rendersi conto di come I.A. già esistenti possano essere usate – se già magari non accade, all'insaputa di noi tutti – per compiere determinati reati, magari nel *cyberspace*; la seconda, per rendersi conto di come, nel giro di pochi anni, le tecnologie si evolveranno rendendo disponibili tipologie di I.A. le quali permettano di compiere reati in modi oggi impossibili, oppure permettano di compiere determinate indagini in modi oggi ancora impossibili».

Solo se sapremo cogliere questa sfida dei tempi, allora, potremo sedere al tavolo delle trattative (a livello europeo, internazionale e, quando servirà, anche bilaterale) come pari o, quantomeno, comprimari, e non come semplici osservatori.

Illustrazione della regolamentazione europea sulla *Mutual Legal Assistance* (MLA) nel *cyberspace*

di Beatrice Fragasso
Dottoranda di ricerca in Diritto penale, Università degli Studi di Milano

Nella relazione che segue cercherò di rilevare quali sono le prospettive della normativa europea ed internazionale in materia di giurisdizione e di acquisizione delle prove elettroniche.

I problemi inerenti all'esercizio della giurisdizione nel *cyberspace* non sono una novità e risalgono agli albori di internet: tali problemi sono tuttavia oggi esacerbati dall'incremento di rapidità del flusso di dati, dall'evoluzione degli strumenti tecnologici virtuali, ma soprattutto dalla *pervasività* dello spazio virtuale.

Se infatti nel 2001 – quando è stata siglata la Convenzione di Budapest[7] – l'obiettivo era di garantire un'adeguata prevenzione e repressione di un piccolo nucleo di reati informatici – riconducibili a nove categorie – oggi non solo le condotte offensive *online* si sono moltiplicate, ma si può dire che praticamente tutti i reati lasciano tracce nel mondo virtuale, ponendo agli organi investigativi il problema di acquisire prove decisive in uno spazio deterritorializzato, sul quale spesso non esercitano la giurisdizione.

In materia di sicurezza informatica, vi sono due piani distinti che possono entrare in gioco: da un lato, i rapporti tra stati sovrani, con i cyberattacchi che possono configurarsi come veri e propri atti di guerra e di violazione della sovranità statale; dall'altro lato, la commissione di reati nello spazio virtuale.

L'identificazione dell'ambito di riferimento è di fondamentale importanza, poiché implica l'applicazione di un *corpus* normativo in luogo dell'altro. In un caso, infatti, si farà ricorso al Diritto internazionale, ed eventualmente allo *ius in bello*. Nel secondo caso, si utilizzeranno gli ordinari strumenti giurisdizionali del processo penale.

Va tra l'altro rilevato che nel concreto sembra sempre più complesso distinguere i due piani. Il rapporto tra cybercriminali e organi governativi di alcuni paesi è ormai sotto gli occhi di tutti. Tuttavia, sia che si tratti di criminali comuni, sia che si tratti di *hacker* al soldo dei Governi, si pone un problema centrale, che è quello dell'attribuibilità e, dunque, dell'accesso alla prova elettronica. Come individuare l'autore del fatto illecito, in un contesto in cui – approfittando della volatilità e frammentarietà dei dati – i criminali possono far rapidamente sparire le proprie tracce?

Ecco che allora la comunità internazionale e l'Unione Europea – e prima ancora gli Stati Uniti – si stanno muovendo lungo una chiara direttrice, che è quella della collaborazione diretta con gli *Internet Service Provider*.

---

[7] Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica, aperta alla ratifica il 23 novembre 2001.

Prima di concentrarci sulle proposte che sono in corso di discussione in ambito europeo e internazionale, può essere utile porre l'accento sull'attuale disciplina dell'accesso ai dati e sulle criticità che sono state riscontrate. Oggi l'accesso ai dati è regolato dai meccanismi di cooperazione giudiziaria, previsti sia dalla Convenzione di Budapest (artt. 23 e 25), sia da fonti dell'UE (tra le tante, possiamo limitarci a ricordare la Direttiva del 2014 sull'Ordine europeo di indagine[8]), nonché da accordi bilaterali sulla mutua assistenza giudiziaria tra l'Unione e gli Stati terzi, come quello con gli Stati Uniti d'America[9] e con il Giappone[10].

Nella prassi, tuttavia, l'acquisizione di prove digitali ha incontrato alcune peculiari criticità. In primo luogo, la lentezza: in un contesto globalizzato in cui i *cyberattacks* sono all'ordine del giorno, i procedimenti di MLA risultano lenti e farraginosi, richiedendo spesso alcuni mesi per la loro implementazione[11]. Le norme che regolano questi meccanismi sono state concepite per le prove fisiche, e prevedono tempistiche di trasmissione inadatte alla velocità con cui le prove digitali si muovono nella rete e possono trasmigrare da uno Stato ad un altro.

In secondo luogo, i meccanismi di assistenza giudiziaria presuppongono un unico Stato di esecuzione. La dispersione delle prove digitali, tuttavia, spesso porta alla moltiplicazione delle giurisdizioni coinvolte. Qual è, allora lo Stato di esecuzione? Lo Stato in cui opera o ha la sede legale il *service provider* che ha accesso alle prove? Oppure lo Stato in cui si trova il *server* dove si trovano le prove, magari diverso dallo Stato del *provider*[12]? E in quest'ultimo caso, come effettuare la scelta qualora, come spesso accade

---

[8] Direttiva 2014/41/UE del Parlamento europeo e del Consiglio, del 3 aprile 2014, relativa all'ordine europeo di indagine penale.

[9] Accordo sulla mutua assistenza giudiziaria tra l'Unione europea e gli Stati Uniti d'America (GU L 181 del 19.7.2003).

[10] Accordo tra l'Unione europea e il Giappone relativo all'assistenza giudiziaria in materia penale (GU L 39 del 12.2.2010).

[11] CYBERCRIME CONVENTION COMMITTEE (T-CY), *T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime adopted by the T-CY at its 12th Plenary (2–3 December 2014)*, disponibile sul sito del Consiglio d'Europa; vd. anche l'*impact assessment* all'*E-evidence package*, *Commission staff working document impact assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings* – SWD/2018/118 final, *passim*; B. KOOPS – M. GOODWIN, *Cyberspace, the cloud, and cross-border criminal investigation*, *in Tilburg Law School Research Paper No. 5/2016*; T. CHRISTAKIS – F. TERPAN, *EU–US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options*, in *International Data Privacy Law*, 2021, Vol. 11, No. 2; nella letteratura italiana vd. M. DANIELE, *L'acquisizione delle prove digitali dai* service provider*: un preoccupante cambio di paradigma nella cooperazione internazionale*, in *Rev. Bras. de Direito Processual Penal*, vol. 5, n. 3, 2019, p. 1280; M. GIALUZ – J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, in *Dir. pen. cont.*, 5/2018, p. 281.

[12] Come accaduto, ad esempio, nel noto caso deciso dalla Corte Suprema, *United States v. Microsoft Corp., 584 U.S (2018)*, in cui l'autorità giudiziaria statunitense aveva chiesto a Microsoft, azienda statunitense, alcuni dati reperibili in un server situato in Irlanda. In particolare, in quella vicenda, Microsoft aveva rifiutato di fornire l'e-mail di un cittadino americano – conservata in un server in Irlanda – dopo aver ricevuto un mandato dall'FBI ai sensi dello *Stored Communications Act* (*section 703*). Il rifiuto aveva aperto una controversia legale, poiché Microsoft sosteneva che l'SCA non copriva i dati conservati al di fuori degli Stati

per ragioni economiche od organizzative, le prove vengano fatte costantemente circolare fra *server* situati in Stati diversi?

In assenza di soluzioni internazionali condivise, ad oggi gli accessi avvengono attraverso una cooperazione informale con i fornitori di servizi, quasi di natura privatistica[13]. Ogni anno, le autorità giudiziarie e le agenzie di *intelligence* dei paesi europei richiedono l'accesso a decine di migliaia di dati su utenti e *account*. In base ad un recente studio condotto da *Eurojust*[14], risulta ad esempio che nel 2020 le richieste inviate dalla Germania agli *Internet Service Provider* (quali, ad esempio, Apple, Facebook. Google e Twitter) siano state 63.561; la Francia ne ha invece inoltrate 43.252 e l'Italia 10.699.

L'inefficienza del sistema emerge plasticamente dall'*Impact Assessment* che ha accompagnato la presentazione delle proposte europee in tema di prova elettronica[15], dal quale si evincono tre dati di rilievo:

(i) più della metà delle indagini effettuate in UE comprende una richiesta di accesso transfrontaliero alle *e-evidence*[16];

(ii) meno della metà delle richieste ai fornitori di servizi vengono soddisfatte[17];

(iii) quasi due terzi dei reati che comportano un accesso transfrontaliero alle prove elettroniche – con le attuali regole europee – non possono essere efficacemente indagati o perseguiti[18].

È proprio l'obiettivo di facilitare l'acquisizione della prova elettronica ad aver ispirato l'elaborazione di alcune proposte normative: il Regolamento e la Direttiva che compongono l'*E-Evidence Package*[19] ed il Secondo protocollo addizionale alla

---

Uniti e che l'FBI avrebbe potuto beneficiare soltanto di meccanismi di cooperazione giudiziaria. Approvato il *Cloud Act*, il governo federale ha ottenuto un nuovo mandato conforme al *Cloud Act*, che sostituiva il precedente. La Corte Suprema ha dunque rigettato il ricorso dichiarando l'irrilevanza della questione proposta.

[13] Così C. BUCHARD, *Regolamento europeo* e-evidence*. Deficitario dal punto di vista dello stato di diritto, superato dalla realtà e a lungo termine in contrasto con gli interessi europei*, in *Eurojus*, 2/2020, p. 201; vd. anche P. DE HERT – C. PARLAR – J. THUMFART, *Legal arguments used in courts regarding territoriality and cross-border production orders: From Yahoo Belgium to Microsoft Ireland*, in *New Journal of European Criminal Law*, 2018, Vol. 9(3), *passim*; I. WALDEN, *Law Enforcement Access to Data in Clouds*, in C. Millard (ed.) *Cloud Computing Law*, Oxford University Press, p. 283 ss.

[14] SIRIUS EU Digital Evidence Situation Report, 3d annual report, 2021, p. 55, disponibile sul sito di *Eurojust*. Il report si riferisce all'anno 2020.

[15] *Proposta di regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale* – COM/2018/225 final - 2018/0108 (COD) e *Proposta di direttiva del Parlamento europeo e del Consiglio recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali* – COM/2018/226 final - 2018/0107 (COD); per l'*impact assessment* vd. *Commission staff working document* – SWD/2018/118 final, cit.

[16] *Commission staff working document* – SWD/2018/118 final, cit., p. 14.

[17] *Ibidem*, p. 15.

[18] *Ibidem*, p. 17.

[19] *Proposta di regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale*, cit.; *Proposta di direttiva recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali*, cit.

Convenzione di Budapest[20]. Questi strumenti si muovono tutti nella medesima direzione, che è quella di garantire agli Stati parte una procedura legale per accedere alle prove elettroniche mediante una richiesta diretta al fornitore di servizi; senza, dunque, alcun coinvolgimento dell'autorità giudiziaria del paese ospitante. In particolare, la proposta di Regolamento dell'UE sull'*E-evidence* prevede due tipologie di richieste: l'ordine di produzione, mirato alla trasmissione dei dati, che deve essere adempiuto nel termine di dieci giorni (sei ore, nei casi di emergenza)[21]; l'ordine di conservazione, finalizzato invece alla custodia dei dati in vista di una successiva richiesta di produzione[22]. In caso di inadempienza, i *provider* possono essere sottoposti a sanzioni pecuniarie[23].

Gli elementi di novità sono molteplici, e corrispondono ad altrettante linee di tendenza della regolazione del *cyberspace* a livello globale.

Innanzitutto, un primo fondamentale elemento di novità consiste nell'obbligo per i fornitori che offrono i loro servizi nell'Unione Europea di designare un rappresentante legale per la ricezione delle richieste e per l'applicazione della normativa[24]. Si assiste dunque ad un tentativo di ri-territorializzare la giurisdizione, prendendo atto che uno dei maggiori ostacoli all'ottenimento delle prove elettroniche, fino ad ora, è consistito nel rifiuto dei *providers* di fornire dati localizzati fuori dalla giurisdizione dello stato richiedente. La stessa dott.ssa Nunzia Ciardi – vicedirettrice dell'Agenzia per la Cybersicurezza Nazionale e per anni a capo della Polizia Postale – nel precedente incontro organizzato dalla Fondazione Occorsio raccontava come, ad oggi, sia di fatto impossibile accedere ai dati detenuti da *Telegram*, dato che la società non rende nemmeno nota la sede presso la quale effettuare le notifiche.

In secondo luogo, vi è un superamento della logica centralizzata fondata sulla necessaria interlocuzione tra le autorità dello stato di emissione e dello stato di esecuzione.

Si va dunque verso una disintermediazione, che, se da un lato permetterà un *enforcement* più rapido ed efficiente, dall'altro costituisce un ulteriore capitolo del crescente ruolo assunto dalle società private nella tutela dei diritti fondamentali[25].

---

[20] *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, CM (2021)57-final.

[21] *Proposta di regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale*, cit., artt. 5 e 9.

[22] *Proposta di regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale*, cit., art. 6.

[23] *Proposta di regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale*, cit., art. 13.

[24] *Proposta di direttiva recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali*, cit.

[25] Il dibattito in letteratura è molto ampio. Si vedano, per tutti, V. MITSILEGAS, *The privatisation of mutual trust in Europe's area of criminal justice: The case of e-evidence*, in *Maastricht Journal of European and Comparative Law*, Vol. 25(3), 2018; M. DANIELE, *L'acquisizione delle prove digitali dai* service provider, cit.; A. ROSANÒ, *La "privatizzazione" nello spazio di libertà, sicurezza e giustizia: tre esempi per una tendenza*, in *Il Diritto dell'Unione europea*, 2020, p.179 ss.

Una volta ricevuto l'ordine, infatti, i *providers* dovranno controllare l'eseguibilità degli ordini, sulla base di criteri non molto diversi da quelli ordinariamente utilizzati dalle autorità giudiziarie chiamate ad eseguire le rogatorie e gli Ordini europei di indagine. Tra i criteri vi sono, ad esempio, la verifica circa la manifesta violazione della Carta di Nizza o la manifesta arbitrarietà della richiesta[26].

Una disposizione non dissimile si riscontra tra l'altro nel *CLOUD Act* del 2018[27], l'omologo statunitense del regolamento europeo.

La politica di attribuzione ai fornitori di servizi online di poteri di (*soft*) *enforcement* non è, d'altra parte, un fenomeno nuovo, specialmente per quanto concerne il controllo sui contenuti pubblicati dagli utenti sui *social network*[28]: un compito molto delicato – quello di stabilire cosa è lecito e cosa no, cosa costituisce legittima manifestazione del pensiero e cosa, invece, rappresenta un pericolo per la pubblica sicurezza o una lesione della dignità personale – che corrisponde ad una funzione di bilanciamento di diritti tradizionalmente svolta dagli organi giurisdizionali.

In ogni caso, la via del dialogo diretto con i fornitori di servizi sembra oggi il modello privilegiato in materia di accesso alle prove elettroniche. Il Secondo Protocollo alla Convenzione di Budapest propone uno strumento assimilabile[29] e sono in corso negoziazioni tra Unione Europea e Stati Uniti per garantire meccanismi analoghi per l'accesso transfrontaliero ai dati[30].

Non può essere trascurato, tuttavia, che anche il rapporto diretto con i *service provider* nulla può in relazione ai sistemi di criptazione *end-to-end*, quali WhatsApp, Telegram e Signal.

---

[26] *Proposta di regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale*, cit., art. 14, par. 4 (per l'ordine europeo di produzione) e per 5 (per l'ordine europeo di conservazione).

[27] *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act), H.R.4943 - 115th Congress (2017-2018), disponibile sul sito del Congresso; vd. (2) MOTIONS TO QUASH OR MODIFY: «*A provider of electronic communication service to the public or remote computing service, including a foreign electronic communication service or remote computing service, that is being required to disclose pursuant to legal process issued under this section the contents of a wire or electronic communication of a subscriber or customer, may file a motion to modify or quash the legal process where the provider reasonably believes* […] *(ii) that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government*».

[28] Per una ricognizione dei problemi in materia vd. K. KAESLING, *Privatising Law Enforcement in Social Networks: A Comparative Model Analysis*, in *Erasmus Law Review*, 11, 2018, p. 151 ss.; E. COCHE, *Privatised Enforcement and the Right to Freedom of Expression in a World Confronted With Terrorism Propaganda Online*, in *Internet Policy Review* 7(4), 2018; M.K. LAND, *Against Privatized Censorship: Proposals for Responsible Delegation*, in *Virginia Journal of International Law*, vol. 60-2, 2020, p. 363 ss.

[29] *Second Additional Protocol to the Convention on Cybercrime*, cit., *Section 2 – Procedures enhancing direct co-operation with providers and entities in other Parties*.

[30] Vd. *Decisione del consiglio che autorizza l'avvio di negoziati in vista della conclusione 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*, 21 maggio 2019, 9114/19; vd. anche l'*Addendum to the Recommendation for a COUNCIL DECISION authorising the opening of negotiations with a view to concluding an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters*, 27 maggio 2019, 6102/19 ADD 1; per una panoramica sui contenuti delle negoziazioni vd. T. CHRISTAKIS – F. TERPAN, *EU–US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options*, in *International Data Privacy Law*, 2021, Vol. 11, No. 2, 2021.

In questi casi, infatti, nemmeno il fornitore del servizio può accedere alle chat, poiché le chiavi di decodificazione del messaggio criptato appartengono soltanto al *device* del destinatario del messaggio. Anche qualora, dunque, le autorità giudiziarie riuscissero ad avere accesso al dato, questo sarebbe illeggibile.

La questione è ovviamente legata alla sempre più diffusa consapevolezza dell'opinione pubblica in ordine alla tutela dei dati personali, ma in realtà ha a che fare anche e soprattutto con profili di sicurezza informatica.

Come già nel 2016 affermavano i vertici di Apple nel rifiutare la richiesta dell'FBI di sbloccare l'Iphone di uno dei responsabili dell'attentato di San Bernardino, sviluppare una *backdoor* può mettere a repentaglio la sicurezza informatica di tutti gli utenti e, in quel caso, avrebbe potuto creare un pericoloso precedente legale. Una volta creata una crepa nel sistema, questa può essere infatti facilmente aggredibile da qualsiasi criminale informatico.

Le stesse motivazioni sono state fornite da Telegram per negare al Governo russo le chiavi per decrittare la chat degli organizzatori dell'attentato alla metro di San Pietroburgo del 2017.

La risposta delle autorità, in quel caso, non si è fatta attendere, e l'*app* di Telegram è stata bloccata sull'intero territorio russo[31]. Il blocco è stato tuttavia aggirato facilmente e il 95% degli utenti ha continuato a collegarsi al servizio di messaggistica, grazie a sistemi di VPN facilmente accessibili[32]. Tra l'altro, l'anno scorso, le autorità russe sono tornate sui propri passi, togliendo il blocco su Telegram, senza tuttavia aver ottenuto – quantomeno secondo quanto emerge dalle dichiarazioni ufficiali della società – alcun passo indietro sui temi della *privacy*[33].

È proprio alla luce di questo rapporto contrastato della Russia con le principali piattaforme *online* (non solo Telegram, ma anche Facebook, Youtube, Linkedin) che va letta la proposta di Convenzione contro il *Cybercrime* presentata quest'anno dalla Russia alle Nazioni Unite[34]. Ci sono diversi aspetti che preoccupano nella proposta, che sono già stati evidenziati dalle ONG e dai ricercatori che si occupano di diritti civili e di diritti digitali, e che puntano alla trasposizione nello spazio virtuale di una concezione autoritaria del rapporto tra cittadini ed autorità[35].

Due esempi:

---

[31] Vd. *Telegram, la Russia inizia a bloccare la app in tutto il Paese*, in *Corriere della Sera online*, a cura della Redazione, 16 aprile 2018.

[32] Vd. M. EDWARDS – V. LO BARCO, *Nonostante il divieto, Telegram sopravvive in Russia - ma per quanto tempo?*, in *Global Voices*, 20 novembre 2020.

[33] Reuters staff, *Russia lifts ban on Telegram messaging app after failing to block it*, in *Reuters*, 18 giugno 2020.

[34] *United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*, Draft 29 giugno 2021 (unofficial translation), disponibile sul sito di *Kommersant*, a questo link: https://www.kommersant.ru/docs/2021/RF_28_July_2021_-_E.pdf.

[35] J. HAKMEH, *Russia's Vision for a Cybercrime Treaty*, in *Directions – Cyber Digital Europe*, 16 settembre 2021; T. CLABURN, *Russia tells UN it wants vast expansion of cybercrime offenses, plus network backdoors, online censorship*, in *The Register*, 3 agosto 2021; *Russia: Proposed UN Cybercrime Convention must uphold free speech*, in *Article 19*, a cura della Redazione, 17 febbraio 2022.

(i) si propone un ampliamento della base per l'estradizione, prevedendo che i ventitre crimini informatici elencati non siano mai considerati "reati politici", per i quali le attuali convenzioni internazionali prevedono l'esenzione da estradizione[36];

(ii) la proposta di Convenzione richiede inoltre ai *provider* di fornire "assistenza tecnica", se richiesti dalle autorità – il che sembra far presagire il tentativo di introdurre *backdoor*, da poter sfruttare nell'ambito di procedimenti penali[37].

A tal proposito, non potrebbe essere più distante la posizione espressa dall'Italia nel *Position Paper* presentato alle Nazioni Unite qualche settimana fa[38], in cui si ribadisce la necessità che i diritti civili trovino il pieno riconoscimento nel *cyberspace*. L'esigenza di prevenire e reprimere l'aggressività dei cybercriminali, dunque, non può giustificare la negazione del diritto di libera manifestazione del pensiero e di riservatezza della corrispondenza.

Io credo che la sfida dei prossimi anni, e anzi dei prossimi decenni, sia proprio quella di mantenere, e anzi di rafforzare, le garanzie dei cittadini nello spazio virtuale – garanzie che troppo spesso, ad oggi, sembrano schiacciate dal peso dalle guerre invisibili tra Stati e dagli interessi delle grandi *corporation* a sfruttare i dati personali dei propri utenti.

---

[36] *United Nations Convention*, cit., Article 46, par. 4.

[37] *United Nations Convention*, cit., Article 75.

[38] MINISTERO DEGLI AFFARI ESTERI E DELLA COOPERAZIONE INTERNAZIONALE, *Italian Position Paper on 'International Law and Cyberspace'*, disponibile sul sito del Ministero a questo link: https://www.esteri.it/wp-content/uploads/2021/11/Italian-Position-Paper-on-International-Law-and-Cyberspace.pdf.

DISCUSSIONE A TRE VOCI

Roberto Baldoni, Direttore Agenzia per la Cyber-Sicurezza Nazionale

Laura Carpini, Responsabile unità Cyber/Digital Diplomacy Ministero degli Affari Esteri

Massimiliano Signoretti, Tenente Colonnello Aeronautica Militare Italiana/NATO Cyber Defence Centre of Excellence

Modera Giovanni Salvi, Procuratore Generale Corte di Cassazione e Presidente del Comitato Scientifico FVO

Giovanni Salvi – Vorrei partire da un dato: sei ore è il tempo minimo della cooperazione giudiziaria in materia penale. In sei ore, tuttavia, si effettuano miliardi di transazioni. L'approccio attuale alla giurisdizione e alla cooperazione in materia penale è inadeguato. Come ci ricordava Alessandro Pansa, è un problema che attiene al rapporto tra ordinamento e tecnologia: i due aspetti devono andare necessariamente di pari passo. Allora, di fronte a queste realtà, dobbiamo chiederci se il concetto di giurisdizione abbia ancora un senso e, qualora non ne abbia più, da che cosa sarà sostituito. L'ordinamento ha un *horror vacui*: tutti gli spazi vuoti devono essere riempiti. L'intervento penale richiede, per sua natura, la previsione di una fattispecie di reato, da accertarsi attraverso un procedimento trasparente, che segue regole predefinite. Tutto questo andrà perso? Un problema di questo tipo si pone altresì nell'ambito delle relazioni internazionali. Una cosa è l'enunciazione di principi (la *due diligence*, il diritto di autodifesa), un'altra è l'accertamento, nel caso concreto, della violazione di tali principi.

La questione, allora, è di comprendere come si pone il tema della giurisdizione nazionale – che si basa sul principio di territorialità – rispetto allo spazio virtuale. In via preliminare, è tra l'altro necessario definire cosa s'intenda per spazio virtuale, per *cyberspace*, per poi arrivare a rispondere ad interrogativi più complessi: possiamo applicare il diritto dell'alto mare allo spazio virtuale? Sono due ambiti in qualche maniera assimilabili o si tratta invece di aspetti completamente diversi, rispetto ai quali non vi è nessuna possibilità di applicazione analogica?

Lascerei subito la parola al professor Baldoni, che ci spiegherà innanzitutto che cos'è lo spazio virtuale e a cosa lo possiamo assimilare.

Roberto Baldoni – Ringrazio la Fondazione Occorsio e il Procuratore Generale per questo invito. La domanda che mi pone è un po' la domanda delle cento pistole. Dietro il concetto di giurisdizione c'è il concetto di sovranità digitale, che possiamo definire come la possibilità, per una comunità, di tutelare ed estrarre capacità e ricchezza dai propri dati. Diverse problematiche sorgono in relazione alla sovranità digitale.

La prima, per l'appunto, è la giurisdizione: in che modo è possibile accertare la sussistenza di un reato e le relative modalità di commissione? Come qualcuno ha già notato prima, il problema può essere così posto: se i miei dati sono ospitati in un *server* all'estero e c'è un *breach* di informazioni, come posso assicurare che il reato sia perseguito?

In secondo luogo, c'è un problema di tassazione: se c'è un *service provider* che fa *revenue* all'interno di un certo mercato, dove deve pagare le proprie tasse?

Poi ce n'è un'ulteriore questione, relativa alla sicurezza delle informazioni, che mi tocca da vicino in quanto Direttore Generale dell'Agenzia nazionale per la *Cybersecurity*. Dobbiamo cercare di garantire che le informazioni di cui disponiamo abbiano un elevato livello di confidenzialità ed integrità. La *cybersecurity* è una politica olistica che ha l'obiettivo di proteggere i dati da potenziali attacchi. L'Europa è purtroppo in grave ritardo sulla creazione di *cloud*. All'interno del mercato europeo si è guardato molto alle questioni attinenti alla regolazione e alla competizione interna, senza accorgersi che, nel resto del mondo, si stavano creando dei giganti tecnologici. Vale la pena richiamare qualche caso: il caso Maersk, per esempio, che si porta dietro tutta la problematica dei porti, e, ancora prima, la decisione del '96 della FCC di fare lo *split* di AT&T, che determinò la perdita, per gli Stati Uniti, di un grande *player* internazionale nel settore delle telecomunicazioni. Gli Stati Uniti si sono guardati bene dal ripetere il medesimo errore nel settore digitale, che, infatti, oggi conta numerosi giganti sovranazionali. Il problema, se mai, è opposto: in qualche modo, queste imprese stanno iniziando ad interagire direttamente con le nazioni.

Il Procuratore Generale si chiedeva se la giurisdizione sia destinata a scomparire. Ecco, noi ovviamente lavoriamo affinché questo non avvenga. La legge perimetro di sicurezza nazionale cibernetica ha costituito il primo atto volto a creare un indissolubile legame tra la sicurezza nazionale e la sicurezza cibernetica. Ovviamente, è intervenuta dove poteva, ossia nel settore della sicurezza nazionale, poiché l'art. 4 TUE esclude la sicurezza nazionale dalle materie di competenza europee. La legge ha imposto una serie di misure di sicurezza che ci permetteranno di procedere nella direzione della prevenzione e della deterrenza nell'ambito della *cybersecurity*: prevenzione, ad esempio, in termini di rapidità delle notifiche di incidenti e di scrutinio tecnologico per quanto riguarda il *procurement*. La prevenzione, insomma, in questo momento è il fattore che più ci può proteggere.

Per tornare alle definizioni, allora, la *cybersecurity* è quel tipo di politica che permette di mantenere il rischio *cyber* all'interno di un *range* accettabile dalla società. Questo è quello che noi dobbiamo fare. E, chiaramente, con lo sviluppo tecnologico, il rischio per la sicurezza *cyber* aumenta. Gli attacchi non cesseranno: il nostro compito è di costruire un solido sistema di mitigazione. Ecco, dunque, le parole d'ordine: prevenzione, mitigazione, sviluppo tecnologico. Quest'ultimo aspetto – già citato, prima di me, da Alessandro Pansa e Luciano Carta – è di fondamentale importanza: il fatto, ad esempio, di sviluppare un *cloud* nazionale ci permette di iniziare ad avere dei "cassetti" nazionali a diverso livello di rischio, nei quali inserire le nostre informazioni.

Infine, l'ultimo aspetto fondamentale per il nostro paese è la *workforce*, la forza lavoro. È vero che abbiamo dormito un po' negli ultimi vent'anni, per quanto riguarda

lo sviluppo tecnologico, ma abbiamo dormito ancora di più per quanto riguarda i nostri ragazzi, molti dei quali sono emigrati all'estero. Non erano manovali; si trattava, piuttosto, di battaglioni di ingegneri e di tecnici specializzati. Com'è potuto succedere? Io credo che il nucleo della questione sia rinvenibile in due aspetti molto problematici del nostro Paese: la scarsa qualità del lavoro e la questione salariale. Non possiamo permetterci di subire quotidianamente degli incidenti *cyber* per il fatto che i sistemi informativi non vengono manutenuti in maniera appropriata. Da una ricerca condotta recentemente da Manpower Group emerge che le persone cercano un nuovo lavoro ogni diciotto mesi; molte lo trovano all'estero e da lì non ritornano, per tutti i motivi che tutti sapete.

Ecco, questa è l'altra grande emergenza che in questo momento siamo chiamati ad affrontare: dobbiamo bloccare questo esodo, invertirlo. Possiamo anche elaborare una normativa sulla giurisdizione e avere uno sviluppo tecnologico, ma se non abbiamo forza lavoro abbiamo perso. Senza forza lavoro non può esserci sovranità digitale, poiché questa, per sua natura, necessita di persone che capiscano le problematiche: questo vale nell'A.I., vale nella crittografia, vale nella gestione dei sistemi informativi.

Giovanni Salvi – Il punto che sottolinea il Professor Baldoni è quello della prevenzione e della sicurezza. Siamo tutti d'accordo, questa è la strada principale: la sicurezza va a creare una barriera, è ovviamente ciò che anticipa e risolve larga parte dei problemi. Però io intravedo anche un secondo aspetto. Mi sento un po' come nella favola dello scorpione e della rana: "è la mia natura", non ci posso fare niente, sono un Pubblico Ministero.

Sappiamo che già adesso la reazione da parte degli Stati e delle organizzazioni private, quando subiscono un attacco, non è quella di rafforzare la propria *cybersecurity*: a questo penseranno in un secondo momento. Nell'immediato, piuttosto, reagiscono, distruggono il *server* da cui è partito l'attacco, e intanto entrano nel *cloud* per cercare le informazioni rilevanti, anche se questo è basato all'estero. Non è il futuro, è il presente. Così come lo è il problema della giurisdizione. Abbiamo già avuto un processo in Italia nei confronti di chi, reagendo ad un attacco *hacker*, ha ritenuto di intervenire all'interno di altre giurisdizioni, per acquisire i dati nell'unica maniera in cui è possibile farlo: nell'immediatezza dell'attacco, ricostruendo la rete delle vicende. Hanno aspettato sei ore? Tre mesi? No, lo hanno fatto immediatamente. Questi sono i tempi reali, ma ciò pone il serio tema della giurisdizione.

Veniamo ora alle questioni delicate. Come definiamo lo spazio virtuale? In questo lavoro siamo partiti dall'esperienza italiana a proposito dell'alto mare e, in particolare, dall'affermazione di un principio nuovo nelle relazioni internazionali, ossia la possibilità di esercitare l'*enforcement* della giurisdizione nazionale in alto mare, quando ricorrano alcune condizioni. Abbiamo ordinato sequestri e arresti anche a 200 miglia dalle coste del nostro paese, utilizzando i criteri ordinari di riconduzione della territorialità e le convenzioni di Montego Bay, di Londra e infine di Palermo. Ecco, nello spazio virtuale questi meccanismi non funzionano. Nonostante le pur evidenti analogie, lo spazio virtuale è molto diverso dall'alto mare. L'alto mare ha dei confini chiari, oltre

il quale diventa territorio. Lo spazio virtuale, invece, è un misto continuo di onde elettromagnetiche, di attività eteree, così come di collocazione fisica dei *server*. È difficile rompere questo misto di territorialità e di non territorialità.

Ecco, questo è il tema che ha dovuto affrontare anche l'Italia nelle trattative finalizzate a elaborare una definizione condivisa di *cyberspace* nell'ambito delle relazioni internazionali. Lascerei ora la parola all'ambasciatrice Carpini.

Laura Carpini – Grazie mille di questo invito e buongiorno a tutti i relatori e agli ospiti che ci accompagnano oggi. Sono davvero molto onorata di partecipare a questo incontro e di poter portare – con le limitazioni della "grande nebulosa" di cui adesso parlerò – il punto di vista della struttura che dirigo al Ministero degli Esteri. Si tratta, peraltro, di una struttura molto giovane, nata formalmente con un Decreto del 2019: e questo già dà la misura dell'accelerazione che l'impatto delle nuove tecnologie ha dato alle relazioni internazionali – motivo per il quale la maggior parte delle cancellerie internazionali si stanno dotando di una struttura che si occupa proprio della diplomazia dello spazio cibernetico.

Io partirei, innanzitutto, da un dato significativo. La prima definizione di *cyber* spazio risale ad un romanzo di fantascienza: si tratta di una parola che – quantomeno agli inizi – esulava completamente dall'ambito giuridico e tecnico. Qualche anno fa, nel 2015, il Presidente Obama definì lo spazio cibernetico il *Wild Wild West.* Cosa è successo in questo lasso di tempo? È successo che la creazione di questo nuovo spazio – che è il primo interamente forgiato dalla mano umana – apre davanti a noi il medesimo panorama di fronte al quale si trovarono i pionieri andando nel West nell'Ottocento. In questo ambiente, che non è stato ancora oggetto di una definizione condivisa a livello internazionale, si incrociano interessi e interazioni. Con la pandemia, oltretutto, abbiamo notevolmente aumentato l'utilizzo delle tecnologie e, di conseguenza, l'esposizione agli attacchi *cyber*. Molti degli Stati che aderiscono all'ONU si sono dotati di strutture che si occupano di *cyber* diplomazia, per supportare e affiancare le attività che vengono svolte dalle competenti autorità nazionali. La nostra struttura, ad esempio, sta già lavorando a contatto con l'Agenzia per la *cyber* sicurezza nazionale.

Da un punto di vista internazionale, gli Stati stanno cercando in vari modi di ristabilire "la legge", le regole di comportamento – naturalmente, come sempre accade nel sistema internazionale, con visioni e finalità diverse. Ad oggi, non esiste una definizione condivisa di *cyberspace*. Per alcuni Stati, la discussione su tale concetto può rappresentare l'occasione per rimettere in discussione e cambiare i principi di diritto internazionale ormai consolidati. Per altri – tendenzialmente i paesi occidentali – è invece l'opposto: il tentativo è quello di replicare nello spazio digitale e cibernetico la promozione dei diritti umani, come è stato ricordato poc'anzi dalla dottoressa Fragasso e come abbiamo sottolineato nel nostro Documento di posizione nazionale. L'obiettivo è di scongiurare una situazione di incertezza. Se dovessimo riscrivere oggi delle regole nuove nei rapporti tra Stati, ciò potrebbe voler dire che quelle che stiamo seguendo adesso non sono più valide.

In questo momento di grande incertezza, i documenti presentati dagli Stati si risolvono essenzialmente nell'affermazione di principi, rimanendo su un livello piuttosto astratto. Nel documento presentato dall'Italia abbiamo ribadito il principio della sovranità e l'obbligo di *due diligence*, che si concretizza nel principio per cui ogni Stato deve controllare che cosa succede sul proprio territorio, come anche il Professor Baldoni riferiva poco fa.

In questo contesto, la proposta di convenzione presentata dalla Russia, a cui faceva riferimento poc'anzi il Procuratore Generale, pone delle importanti sfide per i paesi occidentali – che, a differenza della Russia, hanno firmato la Convenzione di Budapest.

A livello di Unione Europea, è stato avviato un vasto programma di regolamentazione, di rafforzamento della resilienza interna e anche – come ricordava il Presidente Pansa – di stimolo all'innovazione; è chiaro, infatti, che la creazione dello spazio cibernetico non solo pone un problema di relazione giuridica fra gli Stati, ma determina anche una grande competizione per il vantaggio tecnologico, poiché chi avrà il vantaggio tecnologico determinerà anche le regole e le interazioni tra Stati. Lo sforzo dell'Unione Europea – sulla scia del successo della regolamentazione sui dati personali – è ora quello di incidere anche in questo settore: pensiamo al regolamento sull'intelligenza artificiale, alla Direttiva NIS 2, al Digital Services Act, al Digital Markets Act, all'E-evidence package. L'obiettivo è di valorizzare tutta la potenza di uno tra i mercati più grandi del mondo – nonché uno tra i maggiori produttori di dati – in modo da influenzare anche la disciplina del *cyberspace*.

Questo, quindi, è in sintesi il quadro in cui ci muoviamo. È un quadro in divenire, diviso, come già accennava il Procuratore Generale. Si tratta anche di un quadro molto "condizionante": d'altra parte, trattandosi di una disciplina in divenire, abbiamo la possibilità di incidere su di essa e plasmarla. Per questo motivo, abbiamo bisogno di una buona dose di intraprendenza e di ottimismo e di sviluppare competenze interne. Il lavoro che sta facendo la Fondazione Occorsio è molto importante e va in questa direzione: è proprio grazie alla lente giuridica e all'*expertise* che potremo riuscire a portare in sede internazionale un apporto più ricco, in modo da aiutare la comunità internazionale a trovare delle strade che possano permetterci di risolvere problemi di portata enorme. Grazie a tutti.

Giovanni Salvi – Il lavoro che è stato fatto dai centri di eccellenza della NATO è davvero straordinario. Il manuale Tallinn – di cui è in preparazione la terza edizione – affronta in maniera efficace i temi della giurisdizione e del diritto *ad bellum* e *in bello*. Chiederei dunque al Colonnello Signoretti di indicare quali sono i profili più delicati e problematici che i redattori del Manuale hanno dovuto affrontare nella definizione del rapporto tra ambiente virtuale e principi di diritto internazionale.

Massimiliano Signoretti – Vorrei anzitutto ringraziare, in apertura, Sua Eccellenza il Procuratore Generale della Corte di Cassazione, dr. Salvi e la Fondazione

Occorsio, per questa straordinaria opportunità di approfondimento di temi estremamente complessi e di attualità, quali l'esercizio della giurisdizione nazionale nel *cyberspace*, il Diritto internazionale, l'lntelligenza Artificiale (I.A.).

Il Diritto internazionale è un sistema normativo flessibile. È stato studiato ed è stato concepito per essere adattabile nel tempo, anche alle nuove tecnologie. Si pensi ad esempio alla previsione dell'art. 36 del I Protocollo Addizionale alle Convenzioni di Ginevra che impone agli Stati, nello studio, messa a punto, acquisizione o adozione di una nuova arma e di nuovi mezzi o metodi di guerra, di verificare che il loro impiego sia conforme ai principi del Diritto Internazionale e del Diritto Internazionale Umanitario in particolare.

Nell'odierna conferenza cercherò di offrire una prospettiva internazionalistica, che origina da un'esperienza pluriennale presso il NATO *Cooperative Cyber Defence Centre of Excellence* (CCDCOE), anche nella direzione del corso di Diritto internazionale applicabile alle Operazioni *Cyber*. Pertanto, il punto di vista del presente intervento è quello dell'attività degli Stati nello spazio *cyber*.

Chiaramente la NATO è un'organizzazione che, per un'esigenza di standardizzazione in vista della condotta di operazioni militari alleate integrate, tende a fornire definizioni. Anche la definizione del *cyberspace* è, infatti, contenuta in pubblicazioni dottrinali della NATO e in particolare nella AJP 3.20 *Allied Joint Doctrine for Cyberspace Operations*. A questo proposito, una rappresentazione tipica del *cyberspace* lo raffigura come una dimensione strutturata su tre livelli (o strati): livello fisico, logico e sociale – a sua volta formato da cinque componenti: componente geografica, delle infrastrutture di rete, della rete logica-informatica, della *cyber* persona o identità virtuale; delle persone fisiche e organizzazioni. Evidentemente, il focus della NATO è principalmente sugli effetti che possono derivare, o che l'Alleanza può realizzare, attraverso la condotta di designate operazioni *cyber*, per il conseguimento di un obiettivo militare o politico.

Per quel che riguarda, in particolare, il tema dell'I.A., il 21 ottobre 2021 i Ministri della Difesa dei paesi dell'Alleanza hanno approvato una strategia NATO sull'I.A.[39]. La NATO vede nell'I.A. non solo una minaccia in grado di trasformare gli scenari, presenti e futuri, delle operazioni militari, ma anche un'opportunità per rafforzarne il vantaggio tecnologico a supporto dei tre compiti chiave della NATO (difesa collettiva, gestione delle crisi, sicurezza cooperativa). E in questo senso va vista la costituzione di una nuova struttura dell'Alleanza, la *Defence Innovation Accelerator for North Atlantic* (D.I.A.N.A.), un'agenzia simile alla *Defense Advanced Research Projects Agency* (D.A.R.P.A.) statunitense, per lo sviluppo e l'impiego di nuove tecnologie per applicazioni militari.

Per quanto riguarda l'I.A., si è accennato che in essa la NATO vede non solo una minaccia, ma anche un'opportunità. Similmente, il Comitato Internazionale della Croce Rossa (CICR) – un'altra voce importante in questo campo – non è contrario in principio alle nuove tecnologie di guerra. Alcune tecnologie militari, come quelle che consentono

[39] Un riassunto della strategia è disponibile sul sito della NATO, a questo link: https://www.nato.int/cps/en/natohq/official_texts_187617.htm.

una maggiore precisione negli attacchi, si ritiene possano aiutare le parti in conflitto a ridurre al minimo le conseguenze umanitarie della guerra, in particolare sulla popolazione civile, e a garantire il rispetto delle regole di condotta delle ostilità. Evidentemente, così come per qualsiasi nuova tecnologia bellica, le tecnologie di precisione non sono di per sé risolutive e le conseguenze umanitarie sul campo dipenderanno dal modo in cui le nuove armi vengono utilizzate nella pratica. Pertanto, come evidenziato nel documento del CICR sull'I.A. del marzo 2021 non si ravvisa una connotazione necessariamente negativa per quanto riguarda l'applicazione dell'I.A. ai conflitti armati[40].

Venendo più da vicino alla questione della giurisdizione, quando il tema è il *cyberspace*, il richiamo è immediatamente alle reti, ai *cloud*, a fenomeni di trasmissione di dati che avvengono in uno spazio non ben definito. In realtà il funzionamento dei *cloud* dipende da un insieme di infrastrutture, di cavi, sia terrestri che sottomarini, di servers, di *data storage systems* e di numerosi altri dispositivi. Sicuramente e necessariamente anche grazie a connessioni tra diversi sistemi, che includono applicazioni, dati e protocolli che consentono lo scambio dei dati attraverso quello che abbiamo chiamato il livello fisico del *cyberspace*. Ma in particolare, e ciò è di sicuro rilievo ai fini dell'individuazione della giurisdizione sulle attività nel *cyberspace*, tutto ciò avviene grazie ad un insieme di infrastrutture fisiche e di sistemi che si trovano nel territorio degli Stati e sui quali gli stessi Stati esercitano la giurisdizione, anche prescrittiva e regolamentare. E indubbiamente gli Stati esercitano la propria giurisdizione anche sugli individui che conducono le operazioni *cyber*, sulle attività stesse, sugli effetti che queste operazioni producono. Oltre alla giurisdizione sul livello o strato fisico del *cyberspace*, il principio di sovranità conferisce agli Stati il diritto di controllare anche taluni aspetti del livello logico del *cyberspace* all'interno dei loro territori. Ad esempio, uno Stato può richiedere ai fornitori di determinati servizi digitali l'impiego di particolari protocolli crittografici per garantire comunicazioni sicure tra web server e browser.

Diverse sono le teorie per quanto riguarda l'esercizio della giurisdizione sulle operazioni *cyber*. Una di queste teorie che ci riguarda più da vicino è la teoria degli effetti: a prescindere dal luogo di origine di un'operazione *cyber* o dal luogo dove si completa la condotta, uno Stato che risenta degli effetti di questa operazione avrebbe titolo ad esercitare la propria giurisdizione. Tuttavia, un conto è affermare la giurisdizione in principio, diverso il suo esercizio effettivo, complicato dalla natura transfrontaliera e globale dell'attività *cyber*.

Gli Stati, in generale, sono liberi di condurre operazioni cibernetiche nel *cyberspace*, con il limite (o divieto) – salvo eccezioni – rappresentato dalla condotta di operazioni *cyber* che violino la sovranità di un altro Stato (principio di sovranità). Questa regola si applica alle sole relazioni tra Stati (o quando la condotta sia comunque attribuibile allo Stato). Pertanto, un attore non statuale non potrebbe violare con un operazione *cyber* la sovranità di uno Stato, ma potrà, semmai, violare le norme penali

[40] Vd. CICR, *Autonomous weapons: The ICRC remains confident that states will adopt new rules*, disponibile sul sito del CICR a questo link: https://www.icrc.org/en/document/icrc-autonomous-adopt-new-rules.

interne di quello Stato, afferenti alla giurisdizione nazionale. La posizione del Manuale di Tallinn è che il principio di sovranità non solo costituisca una regola del diritto internazionale applicabile anche al contesto *cyber*, ma che sia anche la norma che più probabilmente si presti ad essere violata dalla condotta di un'operazione *cyber*. E tale violazione della sovranità di uno Stato può verificarsi sia attraverso una violazione della sovranità territoriale (produzione di effetti sul territorio di un altro Stato), sia attraverso un'interferenza o un intervento di uno Stato negli affari interni di un altro Stato (*domaine reservé*), che si configuri come usurpazione di funzioni sovrane. Ed è assolutamente irrilevante, a questi fini, che gli effetti siano provocati con l'impiego dell'I.A. Quello che rimane ancora incerto, è quale debba essere l'entità degli effetti prodotti per qualificare un'operazione *cyber* come una violazione di sovranità.

Quanto al profilo soggettivo della condotta, sul quale si innesta il tema all'I.A., si ritiene che l'I.A. non alteri il nesso tra le conseguenze dell'attività e l'attore (Stato). La circostanza che una capacità *cyber* operi in modo autonomo, infatti, non è determinante per concludere nel senso di una mancanza, in capo allo Stato che quella capacità impieghi, di un intento di provocare le conseguenze che da quell'impiego derivino. Al contrario, sia la programmazione di tali capacità, che il successivo, eventuale impiego, sono riferibili ad una preordinata attività umana. E, nei limiti in cui una decisione sull'impiego di tali capacità autonome in operazioni *cyber* sia riferibile ad uno Stato, l'uso dell'I.A. non sottrae in alcun modo l'operazione dalla portata delle regole in materia di sovranità e intervento. Il nesso rimane invariato. Quindi, sia che uno Stato per la condotta di un operazione *cyber* impieghi un *software* con capacità autonome, o impieghi un programma informatico, per così dire, "convenzionale" (privo di autonomia), il nesso tra le conseguenze e l'autore (Stato) rimarrà inalterato. Evidentemente, l'impiego di capacità *cyber* autonome è certamente suscettibile di complicare tecnicamente il processo di attribuzione della condotta all'attore, ma, laddove supportata dagli esiti di tale processo, la mera circostanza dell'impiego dell'I.A. non varrà ad eliminare l'elemento di connessione soggettiva.

Nel contesto internazionale e domestico c'è ampia evidenza di operazioni *cyber* condotte con capacità autonome, in grado di autodeterminarsi nel *cyberspace* e anche nei teatri operativi convenzionali e di prendere decisioni in base agli stimoli dell'ambiente circostante, anche in assenza dell'interazione di un operatore.

Per la capacità di determinarsi autonomamente nell'ambiente operativo, una problematica comune all'impiego dell'I.A. nella condotta di operazioni *cyber* è rappresentato dalla possibilità di poter prevedere interamente gli effetti e, quindi, le conseguenze del suo impiego. Ciò, evidentemente, ha rilievo ai fini dell'individuazione dell'elemento psicologico eventualmente richiesto dalla norma primaria ai fini dell'integrazione della fattispecie di illecito internazionale realizzato. In altri termini, il ruolo dell'intenzione nel determinare se un'operazione *cyber* che impieghi capacità autonome violi il diritto internazionale dipende dalla presenza, o assenza, dell'elemento psicologico nella norma primaria.

Per quanto riguarda, nello specifico, la norma consuetudinaria internazionale che impone agli Stati di rispettare la sovranità degli altri Stati, atteso che l'intenzione non costituisce un elemento psicologico presente nella norma primaria che impone il rispetto

della sovranità degli altri Stati (anche una violazione involontaria costituisce comunque una violazione), un'operazione *cyber* condotta con capacità di I.A. che provochi degli effetti indesiderati di un certo rilievo ("interferenza") nel territorio di un altro Stato rappresenterebbe comunque una violazione del principio di sovranità e quindi un illecito internazionale.

Diversa è la rilevanza dell'elemento psicologico nel caso in cui un'operazione *cyber* condotta da uno Stato sia talmente grave da configurarsi quale "intervento" negli affari interni di un altro Stato. L'intervento – rispetto alla mera interferenza negli affari interni (o esterni) di uno Stato – è una forma di violazione della sovranità più grave, poiché reca con sé l'elemento psicologico dell'intento coercitivo, rappresentato dal fatto che l'intervento di uno Stato negli affari interni di un altro Stato è diretto a privare lo Stato vittima di funzioni sovrane ad esso riservate (ad esempio il processo elettorale). In assenza di tale elemento psicologico (l'intenzione coercitiva) in capo all'attore statuale che nel condurre un'operazione *cyber* si affidasse all'I.A., in presenza di effetti indesiderati, non si configurerebbe alcun illecito internazionale. La fattispecie "intervento" richiede, per così dire, un "dolo specifico", rappresentato dall'intenzione di costringere la volontà dello Stato vittima. L'elemento psicologico non potrebbe, pertanto, essere integrato laddove l'effetto coercitivo venisse realizzato in maniera non volontaria (indesiderata) da una capacità autonoma in grado di autodeterminarsi. Di conseguenza, in assenza di tale elemento psicologico nell'attore, non si configurerebbe alcun illecito internazionale. Possiamo pensare, ad esempio, ad eventi di recente osservazione per quanto riguarda il tema della pandemia, quali gli attacchi *cyber* che hanno bersagliato i centri di ricerca vaccinale (per quanto il termine attacchi vada correttamente riservato ad operazioni che hanno determinate caratteristiche in termini di gravità delle conseguenze). Tali "intrusioni", spesso, sono risultate finalizzate a carpire e a sottrarre i segreti industriali, scientifici e la proprietà intellettuale collegata allo sviluppo di vaccini per il Covid-19. Laddove un'operazione *cyber* di sottrazione di segreti per lo sviluppo di vaccini venisse condotta impiegando delle capacità autonome (I.A.) e il *software* così programmato producesse anche degli effetti ulteriori e indesiderati rispetto alla mera sottrazione di proprietà intellettuale – quali, ad esempio, la cancellazione dell'intero set di dati della ricerca – determinando, così, l'arresto improvviso del programma di ricerca scientifica e dello sviluppo di quel vaccino, in questo caso l'elemento psicologico dell'intenzione sarebbe assente e non potrebbe, perciò, configurarsi da un punto di vista di diritto internazionale un caso di intervento di uno Stato negli affari interni di un altro Stato. Come detto in precedenza, infatti, l'intervento nel dominio riservato di uno Stato richiede l'elemento psicologico dell'intenzione – intento specifico di privare uno Stato di una funzione sovrana (contrasto ad una pandemia in corso). Nel caso in esame, come in altri simili, attenendo lo sviluppo di vaccini per far fronte a pandemie ad una funzione sovrana dello Stato, sarebbe possibile configurare un'operazione *cyber* come descritta in termini di "intervento" negli affari interni di uno Stato, solo laddove: a) emerga l'elemento psicologico dell'intenzione coercitiva (privazione di funzioni sovrane); b) dietro una simile operazione si celi un paese straniero e, c) la condotta posta in essere sia ad esso riferibile (*attribution*).

Un altro tema, di estrema rilevanza nel dominio *cyber*, è quello della *due diligence*, inteso quale corollario del principio di sovranità e generale standard di condotta richiesto agli Stati nelle relazioni internazionali. Il dovere di *due diligence* degli Stati (per quanto non universalmente riconosciuto) si fonda sul principio generale del diritto internazionale secondo cui gli Stati devono esercitare la "dovuta diligenza" per garantire (o non consentire consapevolmente) che il territorio e le infrastrutture sui quali esercitano la propria sovranità non siano utilizzati per arrecare danno ad altri Stati. Pertanto, uno Stato che abbia la consapevolezza che da un'infrastruttura *cyber* localizzata sul proprio territorio derivino operazioni *cyber* dirette e condotte da un altro Stato che provochino effetti gravi in uno Stato terzo e che non adotti adeguate misure da esso praticabili per fermare o limitare gli effetti di tale attività, si ritiene in violazione del dovere di *due diligence*.

A livello internazionale, il paradigma reattivo che uno Stato ha a disposizione nei confronti di un'operazione *cyber* che violi la propria sovranità è fornito dal diritto consuetudinario e, in particolare, dalle norme sulla responsabilità internazionale degli Stati per atti illeciti internazionali. La gamma di misure in autotutela previste dall'ordinamento internazionale (e concepite come circostanze escludenti l'illecito) spaziano dalle semplici ritorsioni alla *self-defence*, come reazione estrema ad un evento *cyber* che possa qualificarsi come "attacco armato" e che abbia una particolare caratterizzazione in termini di attore, di gravità e natura degli effetti, di oggetto dell'operazione (*target*). Perciò, le misure di reazione o rimedi previsti dall'ordinamento internazionale in caso di attività *cyber* malevole possono essere di livello e intensità differente. Le "ritorsioni", sono misure di reazione che, per quanto non amichevoli, non violano il diritto internazionale e non costituiscono illecito (ad esempio l'espulsione dal territorio di diplomatici del paese che si presume autore della violazione). Diversamente, le "contromisure" sono comportamenti che violano una norma di diritto internazionale, ma possono essere adottate da uno Stato vittima di un'attività *cyber* di grado più intenso che costituisca essa stessa un illecito internazionale (ad esempio, violazione del principio di sovranità). Evidentemente, l'illecito iniziale, di cui le contromisure costituiscono risposta, deve essere attribuibile ad un altro Stato (tecnicamente e legalmente), non a gruppi non statuali o ad individui (a meno che nell' attività dell'individuo o dell'organizzazione non statuale non si rilevino gli elementi della direzione e del controllo da parte di uno Stato).

Con riferimento, infine, alla problematica della risposta giurisdizionale ad illeciti internazionali commessi da uno Stato nel *cyberspace* o attraverso di esso, si ritiene che la risposta al livello di giurisdizione penale nazionale si configuri come necessaria e complementare alla risposta a livello internazionale degli Stati, finalizzata evidentemente (anche) ad un obiettivo di deterrenza della minaccia *cyber* ai vari livelli. L'esame della prassi internazionale conferma l'approccio multilivello.

Quanto alla distinzione tra *cyber defence* e *cyber security*, chiaramente la *cyber security* è un problema comune ad entità sia private che pubbliche (anche della Difesa) e consiste nell'assicurare principalmente la funzionalità dei sistemi ponendo in essere tutte quelle misure che possano garantire, difendere e mantenere tale funzionalità in presenza di attività *cyber* malevole. Diversamente, per *cyber defence* si intende, più

precipuamente, l'attività degli Stati, anche al di fuori dei propri sistemi e delle proprie reti, di previsione, contrasto e neutralizzazione della minaccia.

Per tornare ancora alla questione della risposta giurisdizionale, è possibile guardare alla strategia *cyber* degli USA del 2018 che prevede non solo una difesa attiva – lasciando in disparte ogni considerazione circa le operazioni puramente offensive – ma anche una difesa avanzata (*forward defence)*, nel senso di posizionare *software* di allertamento (e risposta preventiva) nei sistemi avversari già in tempo di pace. La strategia di ingaggio permanente degli USA risulta quindi supportata, anche nel dominio *cyber*, dal posizionamento di capacità cibernetiche nei sistemi avversari. Ciò, con ogni evidenza, pone comprensibili dubbi circa il puntuale rispetto delle norme del diritto internazionale, con particolare riferimento sia al principio di sovranità, che della soglia di avanzamento della legittima difesa preventiva (*anticipatory self-defence*). Ma è evidente che i vari Paesi affrontano in maniera diversa il problema della possibile risposta alla minaccia *cyber*, diversificata a seconda della postura di ciascuno di essi a livello internazionale, del loro *soft* o *hard power*, della diversa capacità di influenza. E, necessariamente, del quadro legale e normativo domestico in cui i vari attori *cyber* nazionali si trovano ad operare, che influenza e informa, inevitabilmente, anche la loro capacità di operare oltre i confini. Grazie per l'attenzione.

Laura Carpini – Vorrei aggiungere che alcuni di questi principi non sono condivisi da tutti in ambito internazionale. Per esempio, non tutti i paesi che hanno fornito un documento di posizione o la propria visione di come si applica il diritto internazionale hanno affermato il principio della *due diligence* nello spazio cibernetico. E questo è un po' l'elemento di nebulosa che rende difficile pensare che si possa arrivare ad una convenzione come quella sul diritto del mare o che si possano applicare in modo speculare i medesimi principi. L'affermazione da parte italiana dell'obbligo della *due diligence* è senz'altro utile ai fini della giurisdizione, ma siamo in una fase in cui il diritto internazionale si sta ancora cristallizzando: per noi i principi descritti dal Colonnello sono validi, ma per altri non lo sono. Questo è parte della sfida.

Sull'aspetto, poi, del diritto del mare, c'è forse un ulteriore elemento di differenza. I paesi occidentali stanno tentando di promuovere una nozione di *cyberspace* avente alcuni profili di territorializzazione, proprio sull'esempio della convenzione di Montego Bay. Adottare rigorosamente tali principi, tuttavia, equivarrebbe ad affermare che non solo chiudiamo il confine delle acque, ma addirittura controlliamo tutte le molecole dell'acqua! Lo spazio digitale è infatti composto da informazione. È una questione di carattere filosofico che mi pongo personalmente e sulla quale non mi sono data ancora alcuna risposta.

Giovanni Salvi – È un quesito molto interessante. E veniamo alla conclusione di questo giro, perché siamo arrivati credo esattamente alle due questioni fondamentali.

Innanzitutto, mi sembra che emerga con forza il problematico rapporto tra pubblico e privato. A ben guardare, si tratta di categorie ormai obsolete: è difficile

considerare private delle *over-the-top companies* che sono in grado di autoregolarsi e di disciplinare tutto ciò che avviene in relazione a se stesse, senza alcuna possibilità che altri intervengano. D'altra parte – se non sono private – è anche difficile definirle pubbliche. Io le ho definite le Nuove Compagnie delle Indie, perché sono dei vascelli armati che navigano nel mare virtuale, pretendendo di regolarne le onde, e che non sono soggette, di fatto, alla sovranità statuale. Si tratta di un problema di non poco conto, poiché queste organizzazioni sono anche in grado di autodifendersi e di stabilire delle regole che valgono per gli altri. L'esempio di Trump è chiarissimo. A me può anche andare bene che abbiano impedito al Presidente degli Stati Uniti di utilizzare in maniera manipolativa uno strumento di comunicazione. Mi preoccupa che questa sia una decisione unilaterale di un organismo che è in grado di bloccare una comunicazione che ormai è divenuta di uso comune.

C'è poi un secondo aspetto che, a mio parere, è davvero il cuore delle nostre riflessioni, e che potremmo così porre: se non c'è la giurisdizione – e la giurisdizione non c'è né ci può essere in questo momento – quel vuoto viene riempito. E allora noi dobbiamo capire da chi e come viene riempito. Quanto al sistema giudiziario, è evidente come i meccanismi di cooperazione siano ormai obsoleti: sei ore per ottenere collaborazione internazionale sono un tempo infinito nello spazio digitale. L'ora è un'unità di misura che nello spazio virtuale non ha senso.

D'altra parte, gli Stati si stanno muovendo sempre di più nell'ottica della reazione immediata, senza che gli elementi di prova che fondano il preteso diritto di difesa siano resi trasparenti e soggetti a controllo. Ci stiamo avviando verso un mondo di conflitti non rivelati. E questo è molto pericoloso, perché può determinare *escalation* non volute e perché comunque sottrae al controllo del pubblico l'esercizio di poteri sovrani.

È ovvio che anche qui il tema della giurisdizione è strettamente connesso, poiché la reazione spesso si fonda su un consenso preventivo, così come previsto dal Protocollo aggiuntivo alla Convenzione di Budapest: si pensi, ad esempio, a quel consenso che si esprime attraverso la creazione di squadre comuni, che permettono agli Stati di interagire senza bisogno di una specifica autorizzazione preventiva.

Ci sono, poi, forme di controllo successivo. Non è detto che la giurisdizione debba operare sempre con gli strumenti della *mutual legal assistance*, attraverso la richiesta di commissione rogatoria e successiva risposta. Io credo che si debbano trovare nuovi spazi, poiché, in caso contrario, gli Stati saranno costretti ad intervenire direttamente. È già successo più volte. Recentemente la Russia ha dichiarato che la reazione di uno Stato in risposta ad un preteso intervento della Russia era da considerare un atto di guerra. Sembra di tornare a Westfalia. Non so se ci conviene.

Che ne dice, Professor Baldoni? Come bilanciamo la prevenzione con la repressione? Ritorno alla favola dello scorpione e della rana.

Roberto Baldoni – Il Procuratore ha toccato un punto che è assolutamente dirimente e su cui si agisce in questo momento in due direzioni. La proposta di Direttiva

NIS 2[41] ha l'obiettivo di introdurre la c.d. *Joint Cyber Unit*, una struttura volta ad incrementare lo scambio informativo tra gli stati europei, semplificando in questo modo le procedure di attribuzione. È importante comunque non farsi grandi illusioni, poiché comunque delle zone franche resteranno.

In ogni caso, se è vero che il *cyber* spazio è costituito da *hardware*, non possiamo non rilevare come la globalizzazione ha avuto effetto anche nelle catene di approvvigionamento, facendo in modo che tutte le infrastrutture siano legate da una ragnatela. Prendiamo l'incidente *SolarWinds*: ad un certo punto, siamo venuti a conoscenza del fatto che alcuni pezzi della catena di approvvigionamento dell'azienda erano in Stati non proprio democratici, per usare un eufemismo. Ecco che, in questi casi, il tema della giurisdizione emerge con forza.

Quanto alla *Joint Cyber Unit*, non dobbiamo dimenticare che il suo ruolo sarà limitato alla sola Europa – così come, d'altronde, tutte le iniziative riconducibili ad Europol. Le problematiche iniziano quando si esce dall'UE; è qui che si sviluppa il conflitto sotterraneo di cui parlava prima il Procuratore.

L'architettura nazionale di *cybersecurity* negli ultimi quattro anni si è sviluppata attorno a quattro *pillars* fondamentali: resilienza, investigazioni, difesa (da intendersi come Ministero della Difesa e NATO), *intelligence.* È all'interno di quest'ultimo *pillar* che possiamo acquisire le informazioni più rilevanti. Tornando alle mie prime osservazioni, ci tengo dunque a ribadire che la prevenzione è di fondamentale importanza, poiché è in questa fase che l'azione dello Stato si può sviluppare in maniera legale.

L'obiettivo, ovviamente, è di arrivare ad una risposta globale, che chiarisca il concetto di giurisdizione nel *cyberspace*. Il problema è che le regole non le decidiamo noi e dobbiamo adattarci alla realtà concreta delle relazioni internazionali, nonostante le sue evidenti imperfezioni. L'Italia negli ultimi anni ha cercato di costruire una solida struttura di monitoraggio e ricerca su questi temi, che ci permette di navigare in un mare di complessità; molte delle persone che fanno parte di questa piattaforma si trovano oggi in questa sala.

Il tentativo di favorire lo sviluppo tecnologico è finalizzato a preservare la nostra indipendenza e la nostra prosperità, fortemente a rischio in questo nuovo mondo.

[41] Proposta di Direttiva del Parlamento europeo e del Consiglio relativa a misure per un livello comune elevato di cibersicurezza nell'unione, che abroga la direttiva (UE) 2016/1148 – COM/2020/823 final (c.d. NIS 2).

I.A. e reati ambientali

di Pasquale Fimiani, Sostituto Procuratore Corte di Cassazione
e Giuseppe Sgorbati, Università degli studi Milano, Bicocca

SOMMARIO: 1. Obiettivi e metodologia. – 2. Area di ricerca. – 3. Svolgimento della ricerca. – *3.1. Le fonti di informazioni disponibili. Il Sistema Avanzato di Monitoraggio Integrato del Territorio previsto dal PNRR. – 3.2. L'efficace utilizzo delle nuove tecnologie nel contrasto degli illeciti ambientali: condizioni.* – 4. Prospettive della ricerca. – 5. I possibili campi di applicazione della ricerca. – **ALLEGATO N. 1 - CENSIMENTO BANCHE DATI**: 1. SISPED. – 2. Albo Nazionale Gestori Ambientali. – 3. MUD. – 4. Catasto Rifiuti ISPRA – 5. Osservatorio Rifiuti Sovraregionale (ORSO). – 6. Catasto Georeferenziato Impianti Rifiuti (C.G.R. Web). – **ALLEGATO N. 2 - QUADRO GENERALE DEI FENOMENI CRIMINALI IN MATERIA DI RIFIUTI**: 1. Premessa. – 2. Le modalità fraudolente.

1. Obiettivi e metodologia.

La prima fase del lavoro del gruppo è servita per inquadrare le questioni da approfondire e per definire le linee operative della ricerca nell'area tematica di competenza (v. *infra*).

Rispetto al duplice profilo generale della ricerca – nuove modalità di commissione dei reati mediante l'uso dell'Intelligenza Artificiale e prospettive innovative del suo utilizzo nel contrasto e nella prevenzione penale –, si è ritenuto di concentrare l'attenzione sul versante repressivo-preventivo in considerazione della natura "materiale" e non "virtuale" di incidenza sul territorio dei reati ambientali.

Quanto alle possibili modalità di commissione di tali reati anche mediante A.I. nella fase preparatoria ed esecutiva (si pensi ad attività di "*bioterrorismo*" realizzate attraverso l'interferenza nei sistemi di gestione informatica di un acquedotto), il gruppo di lavoro ha ritenuto di attendere alcuni primi risultati provenienti dagli altri gruppi, più direttamente interessati a tale versante della ricerca, da cui trarre indicazioni omogenee in tema di comuni nozioni e definizioni e di verifica della concreta possibilità di individuare uno spazio di giurisdizione, anche transnazionale, per l'accertamento e la repressione dei reati.

2. Area di ricerca.

La ricerca si propone di indagare le potenzialità dell'uso degli strumenti di Intelligenza Artificiale in relazione ai **fenomeni di rilevanza penale che interessano la materia ambientale** (tra cui in particolare l'utilizzo abusivo di risorse naturali, i fatti di inquinamento e di disastro, la gestione illecita dei rifiuti).

3. Svolgimento della ricerca.

3.1. Le fonti di informazioni disponibili. Il Sistema Avanzato di Monitoraggio Integrato del Territorio previsto dal PNRR.

Le potenzialità dell'impiego dell'Intelligenza Artificiale sono fortemente condizionate dal livello di disponibilità, sviluppo, accessibilità e integrazione delle informazioni in formato digitale che costituiscono il necessario substrato per l'operatività degli algoritmi.

In materia ambientale, la ricognizione delle fonti esistenti ha evidenziato come tale disponibilità sia ancora ridotta e frammentaria e meriti, di conseguenza, un definitivo impulso. Si è rilevato come esistano nel settore ambientale una significativa quantità di informazioni provenienti da banche dati e sistemi di monitoraggio sia di natura giudiziaria che di natura amministrativa, ma tali dati sono organizzati in maniera settoriale e senza collegamento fra loro.

D'altra parte, l'esperienza investigativa insegna che nell'ambito delle attività di indagine si acquisiscono dati ed informazioni ulteriori, la cui elaborazione complessiva mediante sistemi di Intelligenza Artificiale consentirebbe di tracciare le condotte secondo canoni di prevedibilità, anche preventiva, idonei a consentire un salto di qualità nel campo dell'accertamento giudiziario, anche attraverso puntuali studi di settore.

È stata quindi effettuata una prima ricognizione delle banche dati già esistenti e dalle quali si potrebbero ricavare informazioni che, tramite l'utilizzo dell'intelligenza artificiale, potrebbero essere "lavorate" per supportare le indagini in materia di ambiente (*v. allegato 1*).

Sono state altresì tenute presenti le prospettive di sviluppo dei Sistemi informativi geografici (c.d. GIS: *Geographic Information System*) – applicazioni della geomatica, ossia della disciplina che integra lo studio del territorio e dell'ambiente con l'informatica – nonché di attuazione del REN, il Registro elettronico nazionale per la tracciabilità dei rifiuti istituito dalla legge 11 febbraio 2019 n. 12.

Si è altresì fatto riferimento al repertorio nazionale dei dati territoriali, previsto dall'art. 59 del Codice dell'amministrazione digitale (d.lgs. n. 82/2005) ed al d.lgs. 19 agosto 2005, n. 195 (Attuazione della direttiva 2003/4/CE sull'accesso del pubblico all'informazione ambientale), che ha previsto all'art. 8 una specifica disciplina per la raccolta e la gestione delle informazioni ambientali.

Indicazioni, queste, che trovano il loro sviluppo e completamento nel PNRR - Piano Nazionale Di Ripresa e Resilienza. Le *Missioni*, nelle quali è articolato il Piano, includono i temi dell'innovazione, della digitalizzazione e della promozione dell'ambiente e della giustizia in stretta, sinergica correlazione. In particolare, la Missione M4C2, il cui Piano Operativo è stato definito con il decreto del MiTE del 29 settembre 2021 (G.U. 20 ottobre 2021, n. 251), si propone di sviluppare un *Sistema Avanzato di Monitoraggio Integrato del Territorio*, destinato ad alimentare anche la fase di prevenzione e repressione degli illeciti ambientali rilevabili con tecniche di osservazione terrestre e georeferenziazione (satelliti, aerei).

3.2. L'efficace utilizzo delle nuove tecnologie nel contrasto degli illeciti ambientali: condizioni.

Le nuove tecnologie a supporto delle diverse fasi della protezione dell'ambiente hanno già dimostrato ampiamente la loro efficacia ed efficienza, e rappresentano strumenti fondamentali tanto nel campo della prevenzione degli illeciti ambientali quanto nella fase del loro contrasto.

Occorre considerare come i più moderni strumenti di sorveglianza ed indagine si inseriscano in una catena logica di azioni, basate sostanzialmente e insostituibilmente su operatori qualificati, con competenze e ruoli istituzionali sostanzialmente differenti.

La disponibilità delle nuove tecniche di osservazione terrestre e di analisi di banche dati attraverso Intelligenza Artificiale, presto rese maggiormente disponibili attraverso il PNRR, rendono innanzitutto possibile l'applicazione estensiva di pratiche di sorveglianza informatica e del territorio, intesa come monitoraggio costante mirato all'individuazione precoce di fenomeni potenzialmente critici. Lo *screening* effettato in questa fase di osservazione ed analisi orienta alternativamente, in seguito ad un processo decisionale mirato, verso la prosecuzione delle indagini o il loro abbandono.

Si è ad esempio constatato come l'applicazione di sistemi di Intelligenza Artificiale all'osservazione terrestre è in grado di produrre un numero estremamente elevato di casi da assoggettare a uno *screening* iniziale e successivamente, in casi di "positività", ad indagine / investigazione, necessariamente tramite operatori specializzati in rappresentanza delle Istituzioni interessate.

La tradizionale catena – acquisizione delle informazioni, analisi, indagine-investigazione e, se del caso, repressione – e i relativi attori rimangono alla base dell'architettura del sistema anche nel caso dell'applicazione delle nuove tecnologie, ma sono messi in crisi tradizionali paradigmi relativi agli aspetti tecnici, giuridici e culturali; anche la gestione dei volumi di informazioni prodotte dalle nuove tecnologie rappresenta una nuova sfida da affrontare.

Alcuni aspetti sono cruciali per l'efficace sviluppo di sistemi di sorveglianza ambientale, nella quale l'Intelligenza Artificiale sia applicata all'analisi di banche dati e altri sistemi di gestione delle informazioni oppure all'osservazione terrestre.

In tale prospettiva, l'implementazione di nuove tecnologie, come nel caso della realizzazione del *Sistema Avanzato di Monitoraggio Integrato del Territorio* prevista dal PNRR, dovrebbe essere accompagnata da:

- uno sviluppo culturale ed informativo di tutti gli attori del sistema;
- la messa a disposizione di risorse dedicate adeguate, quali-quantitativamente, a tutti i livelli destinatari delle informazioni prodotte dai nuovi sistemi tecnologici;
- la proiezione dei dati grezzi derivanti dal monitoraggio condotto attraverso le nuove tecnologie sull'effettivo contesto territoriale, sia attraverso l'uso di "dati complementari", sia attraverso la collaborazione strutturale di operatori aventi una conoscenza diretta dei territori;

- il coordinamento stringente di tutti gli attori della catena della sorveglianza sino alla persecuzione dei reati, anche laddove tali soggetti appartengono a diversi corpi dello Stato e comunque della PA;
- l'utilizzo di protocolli condivisi, affinché tutti gli elementi della catena informino le proprie attività funzionalmente al ruolo e alle finalità e peculiarità degli attori posti a valle rispetto al loro ruolo.

In mancanza di tali condizioni vi è il rischio di rendere la produzione dell'informazione fine a sé stessa e scarsamente utile alla strategia globale di contrasto degli illeciti ambientali, con significativo spreco di risorse.

Le riflessioni di tipo generale appena presentate trovano una conferma nelle esperienze sviluppate, attraverso uno specifico progetto di sorveglianza in alcuni contesti territoriali, in cui un accordo preliminare tra gli attori della fase osservazionale e di valutazione preliminare e la Magistratura si è dimostrato tanto necessario quanto efficace.

Proprio queste prime esperienze confermano l'esigenza che l'attuazione del recente decreto del MiTE del 20 settembre 2021, sulla approvazione del Sistema di monitoraggio integrato previsto Missione M2C4 del PNRR, sia informata alle esigenze del sistema giudiziario attraverso l'individuazione:

- di principi condivisi per la ricerca e selezione degli illeciti, sia ove siano impiegati sistemi di analisi e selezione basati su risorse umane, sia ove vengano impiegate tecniche basate su Intelligenza Artificiale;
- dei livelli di selettività con la quale debbono essere prodotte le informazioni, in modo di bilanciare i casi di mancata identificazione (deficit di sensibilità) ed i casi di falsa identificazione (eccesso di sensibilità);
- di modalità e parametri per garantire l'utilizzabilità delle informazioni prodotte in ambito giudiziario;
- di modalità di gestione sicura dei dati prodotti dal sistema, per garantire la non diffusione di informazioni di potenziale rilievo penale;
- di criteri di priorità per la gestione dei casi identificati, al fine di filtrare opportunamente la massa di informazioni generate ed ottimizzare l'impiego delle risorse umane da utilizzare necessariamente nelle fasi di investigazione dei casi proposti dal sistema di rilevamento ed analisi.

Senza l'opportuna attenzione ai punti evidenziati, da dispiegare già nella fase di sviluppo del progetto previsto dalla Missione M2C2 del PNRR, vi è il rischio dell'allestimento di un sistema che, vuoi per aspetti costituivi di tipo tecnico, vuoi per la scelta delle logiche di uso ed analisi dei dati grezzi disponibili, vuoi per carenza nella definizione delle modalità di condivisione dei risultati prodotti, possa essere al di sotto delle sue effettive potenzialità di supporto al contrasto agli illeciti ambientali.

Va tenuto presente che il punto 5 del d.m. 29 settembre 2021 ("*Temi verticali di applicazione del sistema di monitoraggio*") prevede "l'identificazione di illeciti ambientali" "*principalmente attraverso l'uso di telerilevamento aereo o UAV per ispezioni locali, l'uso di satelliti radar ed ottici incrementa la risoluzione temporale di osservazione identificando minime variazioni nella copertura del suolo (es. escavazioni, sbancamenti, cementificazioni, devegetazione, ecc.)*".

Si tratta di un'attività idonea a produrre una pluralità di dati dei quali sarà necessario individuare criteri di analisi ed utilizzo, in sede investigativa e processuale.

4. Prospettive della ricerca.

L'ampiezza ed il carattere sistemico delle sfide da affrontare, tra le quali il perdurante scoordinamento dei sistemi informativi della PA, se non la loro carenza strutturale, la necessità di un vasto impegno di risorse fortissimamente specialistiche necessarie per l'allestimento di un apparato di I.A. capace di affrontarle, nonché la necessità di un coordinamento tra i sistemi di controllo penale e quelli di gestione e prevenzione ambientale, indicano come necessario il confronto con le Istituzioni competenti.

La Fondazione intende quindi promuovere un'azione di studio, all'interno delle Istituzioni dello Stato e del mondo della ricerca, mirata a supportare l'attuazione del *Sistema Avanzato di Monitoraggio Integrato del Territorio* previsto dal PNRR in modo che possa produrre informazioni per il contrasto degli illeciti ambientali anche utilizzando tecniche di Intelligenza Artificiale.

Le aree di studio che possono essere sviluppate sono relative al censimento delle risorse attualmente disponibili nel campo, alla proposta mirata di sviluppo di strumenti operativi basati su Intelligenza Artificiale, alla identificazione delle necessità di sviluppo ed integrazione delle basi di dati e di informazioni digitali relative al campo ambientale, alle tecniche di *screening* e selezione, ai relativi livelli di sensibilità, alle caratteristiche dei dati prodotti dai sistemi di I.A. in relazione alle esigenze della magistratura.

Tale approfondimento può realizzare il duplice scopo di individuare un sistema generale con funzione al tempo stesso di prevenzione e di controllo ambientale.

Quanto al primo profilo, quello della prevenzione dei reati, si può pensare all'utilizzo dell'intelligenza artificiale in funzione predittiva: l'analisi dei dati inseriti può infatti evidenziare connessioni invisibili all'operatore umano (schemi di ripetizione di comportamenti, luoghi di maggiore concentrazione dei reati, tragitti frequentemente battuti dai trafficanti di rifiuti) e consentire un'attività anticipata di contrasto, oggi impossibile.

Quanto al secondo profilo, relativo al controllo e alla repressione dei reati, la realizzazione di una banca dati nazionale in materia di criminalità ambientale può consentire un approccio molto più "selettivo" del materiale rispetto alla consultazione della sola banca dati SIDDA – SIDNA, la quale oltre a includere solo dati relativi al delitto di cui all'articolo 452-*quaterdecies* c.p. (di competenza della DDA), contiene molto "rumore", ossia dati che non pertengono allo specifico tema della criminalità ambientale e che complicano la ricerca.

La validazione di tale sistema ed il suo livello di affidabilità costituiscono una condizione necessaria per l'ingresso nel processo penale dei dati da esso provenienti, quali indizi gravi, precisi e concordanti, rilevanti ai fini della valutazione della prova ai sensi dell'art. 192, comma 2, c.p.p.

In questo ambito la ricerca dovrà confrontarsi con la categoria della utilizzabilità delle prove e con gli istituti processuali di raccolta delle stesse, onde verificarne la adeguatezza rispetto ai sistemi di acquisizione mediante l'algoritmo dell'Intelligenza Artificiale, anche in considerazione della tutela delle garanzie e dell'esercizio del diritto di difesa e del controllo giudiziale delle prove raccolte.

Il contributo che le professionalità dei partecipanti al gruppo possono fornire riguarda:

– quanto alla componente magistratuale, indicazioni sugli elementi fattuali che i sistemi di I.A. dovrebbero analizzare per fornire supporto alle Procure nella fase investigativa, per consegnare al giudizio una prova dei reati ambientali affidabile ed utilizzabile, nonché per quantificare e ricercare i relativi profitti, nella prospettiva sia nazionale, che sovranazionale, tenendo presente, per quest'ultima, il perimetro applicativo della Convenzione di Palermo;

– quanto alla componente di polizia giudiziaria, la circolarità delle prassi e delle esperienze sulle problematiche investigative, sulle fonti informative e sulla cooperazione di polizia nell'accertamento dei reati ambientali;

– quanto alla componente degli organi di controllo e di gestione, indicazioni sui profili amministrativi ed organizzativi della gestione e prevenzione dell'ambiente.

5. I possibili campi di applicazione della ricerca.

I possibili campi di applicazione della ricerca per l'applicazione della I.A. sono stati così individuati:

a) individuazione dei fenomeni illeciti, di utilizzo abusivo delle risorse ambientali e di grave inquinamento ambientale, mediante monitoraggio del territorio tramite:

– sistemi di sorveglianza avanzata (SAT e altro);
– utilizzazione dei droni anche a fini di documentazione investigativa;
– altre possibili macchine utili per la ricerca intelligente della prova;
– utilizzazione dei dati esistenti in banche dati aggregate, in fonti aperte e nei molteplici sistemi di rilevamento.

b) gestione illecita dei rifiuti, con particolare riferimento:

– al traffico anche internazionale di rifiuti;
– al loro utilizzo illecito negli impianti;
– alla falsa classificazione nei certificati e nei documenti di accompagnamento;
– alla realizzazione di pratiche cartolari fittizie per mascherare l'illecita destinazione.

In questo settore specifico potranno essere usati i sistemi di elaborazione di informazioni provenienti dalle fonti strutturate e non sopra indicate, tra cui ad esempio

– nel campo specifico – le informazioni sui trasporti terrestri e marittimi, la localizzazione e le rotte delle navi commerciali (*v. allegato 2* per un appunto riepilogativo dei fenomeni criminali in materia di rifiuti).

c) inquinamento delle acque, anche internazionali, al fine di risalire all'origine di gravi fatti di possibile rilevanza transnazionale. In tale settore sarà possibile l'utilizzazione delle fonti di cui al punto a).

d) analisi di impatto sanitario, ai fini di supportare l'accertamento dei reati di disastro ambientale (art. 452-*quater* c.p.) e di quello di disastro sanitario di prossima introduzione (art. 445-*bis* c.p., previsto dal d.d.l. Camera n. 2427 presentato il 6 marzo 2020 e in corso di esame). I dati così raccolti possono essere utili anche nella prospettiva di un loro utilizzo per il recupero del territorio.

e) bonifiche dei siti. In tale ambito, appare evidente la mancanza di un monitoraggio multidisciplinare in cui si analizzino sinergicamente:

– le serie storiche dei monitoraggi effettuati dalle Agenzie regionali per l'ambiente e dal soggetto obbligato alle operazioni di messa in sicurezza e bonifica;
– i documenti di valutazione di rischio;
– eventuali studi di impatto sanitario;
– documenti relativi alla qualità delle acque superficiali e sotterranee;
– studi relativi ai c.d. "valori di fondo naturale";
– verifiche in ordine all'utilizzo, nella zona interessata dall'inquinamento (soprattutto delle falde acquifere sotterranee), di pozzi utilizzati per fine irriguo o per allevamento del bestiame;
– nonché studi effettuati da enti specializzati (come il CREA) che analizzino gli effetti di sostanze inquinanti (organiche e inorganiche) nella catena alimentare.

Allegato n. 1
Censimento banche dati

1. SISPED[42].

Il Ministero dell'Ambiente e della Tutela del Territorio e del Mare (MATTM), ora Ministero della Transizione Ecologica (MTE), in linea con quanto previsto dall'art. 50 del Reg. UE 1013/2006, ha istituito un sistema informatico[43] di raccolta dati sulle spedizioni transfrontaliere di rifiuti autorizzate dalle autorità competenti, da implementare, a cura delle Autorità di Controllo (AC), al termine degli interventi eseguiti.

Il sistema, nello specifico, raccoglie i dati relativi alle spedizioni, autorizzate con procedura di notifica ed autorizzazione preventiva scritta, anche al fine di consentire la pianificazione delle ispezioni da parte degli Organi di Controllo (OC), i cui esiti consentono la redazione dell'allegato IX del predetto Regolamento[44].

2. Albo Nazionale Gestori Ambientali.

L'Albo in parola è stato istituito dal d.lgs. n. 152/2006 (T.U.A.) e succede all'Albo nazionale gestori rifiuti disciplinato dal d.lgs. n. 22/1997[45].

Come noto, ai sensi dell'art. 212 del predetto testo unico, il trasporto dei rifiuti è sottoposto ad autorizzazione che si realizza con l'iscrizione al predetto Albo, ovvero con l'iscrizione delle imprese in differenti registri in considerazione della tipologia, della destinazione e del quantitativo di rifiuti trasportati, nonché delle relative modalità di spedizione[46].

Il trasporto è, tra le varie fasi dell'intero ciclo, quella più delicata, in quanto l'illegale smaltimento e gestione avviene quasi sempre in tale contesto. Pertanto, appare

---

[42] Sistema informatico di raccolta dati per le ispezioni sulle spedizioni di rifiuti autorizzate con procedura di notifica ed autorizzazione preventiva scritta. Cfr. manuale operativo disponibile sul sito del MTE: https://www.minambiente.it/sites/default/files/archivio/allegati/rifiuti/manuale_operativoSISPED_vers1.0.pdf.

[43] Cfr. l'apposita pagina sul sito del Ministero della Transizione Ecologica https://www.minambiente.it/pagina/sisped.

[44] Attraverso l'indicazione del numero: *a)* delle ispezioni, compresi i controlli fisici, degli stabilimenti, delle imprese, di intermediari e commercianti collegati alle spedizioni di rifiuti; *b)* delle ispezioni di spedizioni di rifiuti, compresi i controlli fisici; *c)* delle presunte illegalità riguardanti imprese, intermediari e commercianti in materia di spedizioni di rifiuti; *d)* delle presunte spedizioni illegali accertate nel corso di tali spedizioni; *e)* di illegalità accertate ad indagine giudiziaria conclusa, nei limiti della loro ostensibilità.

[45] È costituito presso il MATTM (ora MTE) ed è articolato in un Comitato Nazionale, con sede presso il medesimo Dicastero, e in Sezioni regionali e provinciali, con sede presso le Camere di commercio dei capoluoghi di regione e delle province autonome di Trento e Bolzano.

[46] L'iscrizione all'Albo, che consente il trasporto su tutto il territorio nazionale, si concretizza in un atto autorizzativo che riporta rispettivamente: *a)* il tipo di rifiuto trasportabile; *b)* il quantitativo annuo autorizzato; *c)* le targhe dei veicoli che possono essere utilizzati per trasportare i rifiuti; *d)* eventuali prescrizioni particolari.

particolarmente delicato e rilevante il sistema di controllo di tale trasporto, finalizzato a prevenire e reprimere i più gravi illeciti ambientali.

3. MUD[47].

Il modello in rassegna è stato istituto dalla legge n. 70/1994 e dal 1996 ad oggi rappresenta la principale fonte di informazione in merito alla produzione, gestione, trasporto dei rifiuti speciali ed urbani a livello nazionale.

Le Camere di Commercio raccolgono le dichiarazioni presentate dai soggetti obbligati, le informatizzano per la trasmissione agli enti competenti (Catasto Nazionale, Agenzie Regionali per l'Ambiente, Province, organi di controllo) e predispongono una raccolta statistica articolata su base provinciale.

Sono tenuti alla presentazione della comunicazione produttori e gestori di rifiuti speciali, Comuni, Consorzi e Comunità Montane per le raccolte di rifiuti urbani e assimilabili, Consorzi, gestori di veicoli fuori uso e produttori di apparecchiature elettriche ed elettroniche[48].

Il portale consente di ricercare e consultare le dichiarazioni MUD presentate a partire dal 2005 dai soggetti obbligati[49] e di estrapolare visure ed elenchi di dichiarazioni.

4. Catasto Rifiuti ISPRA[50].

Il Catasto dei rifiuti è stato istituito dall'art. 3 del D.L. n. 397/1988. L'articolazione e le funzioni del Catasto sono individuate dall'art. 189 del D.Lgs. n. 152/2006.

Il Catasto è organizzato in una Sezione nazionale[51], presso l'Istituto Superiore per la Protezione e la Ricerca Ambientale (ISPRA), e in Sezioni regionali o delle Province autonome di Trento e di Bolzano, presso le Agenzie regionali e delle Province autonome per la protezione dell'ambiente.

---

[47] Modello Unico di Dichiarazione Ambientale. Cfr., in particolare, il sito https://muda.infocamere.it/Muda/.

[48] Nel corso degli anni sono variati i soggetti obbligati alla presentazione e i dati da comunicare: dal 2013 la trasmissione del MUD è esclusivamente telematica, fatta eccezione per i piccoli produttori di rifiuti.

[49] Circa 400 mila ogni anno.

[50] Cfr. il seguente indirizzo sul sito dell'ISPRA: https://www.catasto-rifiuti.isprambiente.it/index.php?pg=.

[51] La Sezione nazionale del Catasto contiene le seguenti banche dati:
a) Rifiuti urbani (produzione, raccolta differenziata, gestione e costi di gestione dei servizi di igiene urbana) Banche dati;
b) Rifiuti speciali (produzione e gestione) Banche dati;
c) Elenco nazionale autorizzazioni Banche dati.
Le banche dati organizzano le informazioni acquisite ed elaborate dalla sezione nazionale del Catasto Rifiuti con il contributo delle sezioni regionali e provinciali e, in generale, di tutti i soggetti pubblici detentori dell'informazione, nonché attraverso l'elaborazione del Modello Unico di Dichiarazione ambientale (MUD). I dati, pubblicati con cadenza annuale ai sensi dell'art. 189, comma 6, del D.Lgs. n. 152/2006, sono liberamente consultabili e scaricabili.

L'ISPRA ha organizzato la Sezione Nazionale per via informatica, attraverso la costituzione del Catasto telematico, che intende fornire un quadro conoscitivo completo, costantemente aggiornato e facilmente accessibile in materia di rifiuti.

5. Osservatorio Rifiuti Sovraregionale (ORSO).

ORSO è un'applicazione *web-based*, utilizzata in sedici Regioni[52], per la gestione completa delle informazioni richieste annualmente ai Comuni per la produzione e gestione dei rifiuti urbani e ai soggetti gestori degli impianti per i rifiuti ritirati e trattati, in sostituzione della compilazione e dell'invio di schede cartacee. L'uso dell'applicativo per gli impianti è parallelo alle dichiarazioni MUD; per i Comuni, l'applicativo produce il modello di dichiarazione MUD compilato, per la successiva trasmissione alle Camere di Commercio.

Le Regioni, aderenti attraverso una apposita convenzione al sistema, lo utilizzano in forma diretta o indiretta tramite le proprie ARPA o altri soggetti da esse individuate.

Il sistema, di proprietà di ARPA Lombardia e di ARPA Veneto, è gestito da ARPA Lombardia.

L'applicativo si pone come sistema condiviso e omogeneo per la raccolta dati, con le finalità statistiche previste, in particolare, dall'art. 205 del D.Lgs. 152/2006 e dalle specifiche normative regionali in materia.

---

[52] Riferimenti alla implementazione di O.R.SO. nelle 16 Regioni aderenti possono essere raggiunti ai seguenti *link*:

1. Lombardia (https://orso.arpalombardia.it/),
2. Veneto (https://www.arpa.veneto.it/temi-ambientali/rifiuti/o.r.s.o/applicativo-web-201co.r.so201d-2013-osservatorio-rifiuti-sovraregionale);
3. Marche (https://www.arpa.marche.it/o-r-so);
4. Umbria (https://www.arpa.umbria.it/pagine/rifiuti-urbani);
5. Friuli-Venezia Giulia (https://www.regione.fvg.it/rafvg/cms/RAFVG/ambiente-territorio/tutela-ambiente-gestione-risorse-naturali/FOGLI.A.2/FOGLI.A.32/);
6. Emilia-Romagna (https://www.arpae.it/it/temi-ambientali/rifiuti/dati-rifiuti/banche-dati/applicativo-orso);
7. Valle D'Aosta (https://www.regione.vda.it/osservatoriorifiuti/Applicativo_orso/default_i.aspx);
8. Toscana (https://www.arrr.it/o.r.so);
9. Abruzzo (https://www.regione.abruzzo.it/content/osservatorio-regionale-rifiuti);
10. Basilicata (https://www.egrib.it/applicativo-web-orso-osservatorio-rifiuti-sovraregionale/);
11. Molise (https://www.arpamolise2.it/RIFIUTI/o-r-so/);
12. Liguria (https://www.arpal.liguria.it/tematiche/rifiuti.html);
13. Campania (http://orr.regione.campania.it/index.php/o-r-so.html);
14. Piemonte (https://trasparenza.regione.piemonte.it/documents/97326/26915900/DGR+51-8662+del+29-03-2019/a1744248-b37a-48c4-bf2a-1ad3ae0111bf;jsessionid=5880293182E15346B8CE64EF00662E88.jvm1,%20https://yucca.smartdatanet.it/intro/#/)
15. Lazio (https://www.regione.lazio.it/rl_rifiuti/?vw=contenutiDettaglio&cat=1&id=1329);
16. Sicilia (https://www.regione.lazio.it/rl_rifiuti/?vw=contenutiDettaglio&cat=1&id=132).

L'obiettivo principale è quello di rappresentare un punto di riferimento unico sia per gli Enti, Amministrazioni e soggetti pubblici che la normativa individua, a vario titolo, quali responsabili del trattamento e della gestione dei dati sui rifiuti, sia per gli *stakeholder* che operano nel medesimo settore.

I dati contenuti in ORSO, per quanto riguarda le Regioni aderenti, sono utilizzati da ISPRA per la compilazione delle pertinenti informazioni del Catasto Nazionale dei Rifiuti.

6. Catasto Georeferenziato Impianti Rifiuti (C.G.R. Web)[53].

Il C.G.R. Web[54] è un *database* condiviso da Regione e Province lombarde, istituito nella prospettiva di accumulare in un unico archivio informatizzato i dati tecnici, amministrativi e geografici relativi agli:

a) impianti autorizzati ad effettuare operazioni di gestione dei rifiuti ai sensi degli artt. 208, 209, 211, 214, 215, 216 e 29-*sexies* del D.Lgs. 152/2006;

b) impianti a fonte rinnovabile alimentati anche parzialmente da "biomasse rifiuti" (D.Lgs. n. 387/2003);

c) impianti autorizzati al trattamento in deroga dei rifiuti liquidi negli impianti di depurazione acque reflue urbane, ai sensi dell'art. 110 del D.Lgs. 152/2006.

Il C.G.R. è implementato dagli Enti competenti al rilascio delle autorizzazioni stabiliti dalla Legge regionale n. 26/2003 (Regione Lombardia e Province).

Il Catasto, consultabile liberamente[55], contiene, inoltre, l'applicativo "*Viewer Criteri Localizzativi*"[56], il quale permette di accedere alla cartografia relativa alle aree idonee e non idonee alla localizzazione degli impianti di trattamento dei rifiuti.

L'implementazione del C.G.R. prevede nel tempo di trasferire in unico *database* regionale i contenuti delle diverse banche dati utilizzate dalle singole Autorità competenti. Attualmente, sono resi disponibili i dati relativi a inceneritori e discariche in esercizio.

Per completezza, si citano, da ultimo, le banche dati fiscali[57] e/o quelle di polizia, per le quali occorre avviare le opportune riflessioni in ordine alle limitazioni imposte dalle stringenti previsioni normative in tema di *privacy*, avuto riguardo alle concrete

---

[53] Per una descrizione generale del catasto, cfr.: https://www.regione.lombardia.it/wps/portal/istituzionale/HP/DettaglioServizio/servizi-e-informazioni/Enti-e-Operatori/Ambiente-ed-energia/Rifiuti/ser-catasto-impianto-rifiuti-online-versione-pubblica-ambcatasto-impianti-rifiuti-online-versione-pubblica/catasto-impianti-rifiuti-online-versione-pubblica.

[54] Cfr. http://www.cgrweb.servizirl.it/menu.do?method=homeCgr.

[55] Cfr. http://www.cgrweb.servizirl.it/.

[56] Cfr. http://www.cgrweb.servizirl.it/menu.do?method=criloc.

57 Cfr. l'audizione del Direttore Generale delle Finanze, Prof.ssa Fabrizia Lapecorella, presso la Commissione Parlamentare di vigilanza sull'Anagrafe Tributaria, del 28 aprile 2021, sul tema della "digitalizzazione e interoperabilità delle banche dati fiscali", disponibile all'indirizzo: https://www.finanze.gov.it/it/il-dipartimento/Audizioni-e-interventi/.

modalità di accesso/utilizzo e trattamento (titolarità) delle informazioni ivi contenute, ancorché effettuate avvalendosi di un sistema di intelligenza artificiale.

Allegato n. 2
Quadro generale dei fenomeni criminali in materia di rifiuti

1. Premessa.

La criminalità ambientale rappresenta un fenomeno eterogeneo che ricomprende molteplici manifestazioni illecite quali i reati perpetrati nel settore agroalimentare (c.d. "agrocrimini"), il traffico illecito di rifiuti, l'inquinamento delle acque, dell'aria e del suolo, nonché l'abusivismo edilizio, l'illecito sfruttamento di energie alternative, in particolare l'eolico e il fotovoltaico e, non ultimo, l'"archeomafia", ossia il traffico illecito di opere d'arte e di beni archeologici.

Attesa la sua vastità e l'enorme massa di denaro che gravita intorno ad esso, le organizzazioni criminali appaiono sempre più impegnate a penetrare i diversi settori del comparto ambientale, intravedendo la possibilità, da un lato, di realizzare facilmente considerevoli profitti, dall'altro di riciclare i capitali illecitamente conseguiti.

Tra i vari comparti, quello che negli ultimi anni ha fatto registrare un sensibile incremento degli interessi delle organizzazioni criminali è il traffico illecito di rifiuti, fenomeno che genera sia gravi ripercussioni sull'ambiente, minando la salute dei cittadini e dell'intero ecosistema, che sull'apparato economico nazionale, creando effetti distorsivi sul libero mercato e arrecando grave pregiudizio alle imprese oneste e ai consumatori.

È emersa, in particolare, la propensione delle compagini criminali ad infiltrarsi in tutte le fasi del ciclo dei rifiuti, dalla raccolta al trasporto, fino allo smaltimento, allo scopo di sfruttare le enormi possibilità di profitti che il comparto offre.

Se in origine il fenomeno era circoscritto alle regioni del Sud Italia (Calabria, Campania, Puglia e Sicilia), oggigiorno risulta esteso anche alle aree territoriali del Paese economicamente più floride, quali il Lazio, la Toscana, la Lombardia e il Veneto, dove da tempo si registrano proiezioni criminali.

L'interesse della criminalità organizzata condiziona fortemente il corretto svolgimento delle dinamiche economiche del settore, impedendo ad operatori concorrenti di acquisire quote di mercato e ostacolando di fatto lo sviluppo dell'imprenditoria sana.

Per altro verso, emergono diffuse situazioni di collusione con il sistema imprenditoriale, al fine di ridurre illecitamente i costi necessari allo smaltimento dei rifiuti produttivi, soprattutto quelli pericolosi, che necessitano di specifiche e costose lavorazioni per essere smaltiti legalmente. Per tali attività, infatti, si realizza un più alto margine di profitto sia per l'impresa compiacente, che vede ridursi gli alti costi di smaltimenti dei prodotti di scarto delle proprie lavorazioni, sia per l'organizzazione criminale, che può ottenere "parcelle" elevate per i servizi resi.

A ciò si aggiunge la diffusione di fenomeni corruttivi nell'affidamento dei servizi di gestione dei rifiuti, dovuti sia al comportamento illecito dei responsabili pubblici, sia all'ingerenza delle organizzazioni criminali locali nell'affidamento dei relativi servizi mediante azioni intimidatorie e violente.

Un altro aspetto particolarmente rilevante del fenomeno è rappresentato dal carattere di transnazionalità che riguarda la modalità di commissione dei reati ambientali. Nel corso degli anni, infatti, si è assistito ad un progressivo aumento della propensione dei sodalizi criminali ad esportare i rifiuti, prevalentemente verso i Paesi dell'Africa e dell'Asia, dove le norme a tutela dell'ambiente sono meno stringenti e la manodopera utile per le attività di riciclaggio dei rifiuti si può trovare a basso costo.

Qui i rifiuti vengono riciclati e utilizzati come materia prima per produrre nuovamente beni, destinati soprattutto all'infanzia (giocattoli, biberon, ecc.), che vengono poi reintrodotti nel territorio nazionale e unionale, con gravi rischi per la salute e la sicurezza.

2. Le modalità fraudolente.

Per la realizzazione di crimini ambientali, sono utilizzati diversi sistemi di frode, quali:

(i) la "**triangolazione**" o "**giro bolla**", ossia il **cambio di destinazione del rifiuto**: da smaltimento a recupero, ovvero la declassificazione del rifiuto da "pericoloso" a "non pericoloso". Nello specifico, al rifiuto viene modificato il codice CER (Catalogo Europeo dei Rifiuti) riprodotto nel FIR (Formulario di Identificazione dei Rifiuti), in modo da classificarlo formalmente come non pericoloso ed essere gestito, trasportato e smaltito in maniera illecita, aggirando le normative e le prescrizioni autorizzative del sito al quale il rifiuto è in realtà destinato. In sostanza, il rifiuto che entra con bolla del produttore con un determinato codice, è subito assunto in carico dal centro di stoccaggio con trascrizione nell'apposito registro di carico e scarico dei rifiuti. Successivamente, con nuova bolla dello stesso centro, il medesimo rifiuto, senza subire alcun trattamento ed in alcuni casi senza miscelazione con altri rifiuti, è inviato per lo smaltimento/recupero finale. Tale meccanismo è agevolato dal fatto che risulta poco agevole mettere a confronto i formulari stabilendone il nesso;

(ii) la "**simulazione**" dell'avvenuto **recupero e/o trattamento** dei rifiuti. Il trattamento e/o recupero del rifiuto è solo documentale. Successivamente viene emessa una nuova documentazione accompagnatoria per un materiale diverso rispetto a quello pervenuto all'impianto. Anche in questo caso, si tratta di trasformare "cartolarmente" la disciplina giuridica del rifiuto, in modo da renderla compatibile con la destinazione prescelta. Il programma criminoso viene attuato attraverso la realizzazione di false certificazioni di analisi (oltre che nei documenti di trasporto) e di una serie di attività dirette fittiziamente a far risultare come avvenuti i passaggi presso gli impianti di intermediazione al fine di realizzare un organizzato traffico illecito di rifiuti.

Nel caso specifico del traffico transazionale di rifiuti verso l'estero, le principali condotte illecite possono riguardare:

– la falsa dichiarazione di esportazione verso l'estero dei rifiuti che, in realtà, vengono smaltiti illecitamente in Italia;

– la dichiarazione di esportazione di tipologie di rifiuti diverse da quelle reali, senza sostenere i costi di smaltimento.

È il caso, ad esempio, dei rifiuti speciali non pericolosi, che normalmente dovrebbero essere trattati in Italia ma che, a volte, vengono esportati illegalmente verso Paesi con sistemi sanzionatori meno stringenti ovvero che non dispongono di idonee strutture atte a garantirne la gestione in modo ecologicamente compatibile, con il solo scopo di ridurre i costi derivanti dallo smaltimento.

Per agevolare la consumazione dei delitti ambientali sovente viene fatto ricorso a:

(i) **emissione e utilizzo di fatture false**.

L'imprenditore che opera illecitamente ha necessità di abbassare il reddito imponibile e creare, quindi, costi fittizi attraverso fatture per operazioni inesistenti che, laddove il traffico sia di piccole dimensioni, vengono organizzate in maniera semplice mediante una società cartiera, ovvero attraverso un gruppo di società fittiziamente collegate tra di loro nel caso in cui il traffico sia di più grandi dimensioni.

Nel caso di specie le fatture sono oggettivamente false, in quanto documentano operazioni non realmente effettuate in tutto o in parte.

Le fatture per operazioni inesistenti emesse dalle cartiere sono utilizzate anche per immettere formalmente nel circuito legale delle imprese che intervengono nella filiera di gestione dei rifiuti materiale raccolto da altri soggetti, che operano in assenza delle prescritte autorizzazioni e/o completamente "in nero".

In questa ipotesi, considerato che le operazioni documentate sono intercorse tra soggetti diversi da quelli risultanti formalmente quali parti del rapporto, le fatture sono soggettivamente false. Il tutto, in ogni caso, al fine di evadere le imposte dirette, l'IVA e, eventualmente, i dazi doganali, nei casi di coinvolgimento di altri Paesi.

Di norma tali società cartiere non presentano le prescritte dichiarazioni, non istituiscono un apparato contabile, non versano le imposte e hanno una durata breve (c.d. imprese apri e chiudi).

Talvolta, nel flusso cartolare sono interposte imprese "filtro" che si presentano come regolari sotto l'aspetto amministrativo-contabile e fiscale, ma sono costituite con lo scopo di rendere più complessa l'individuazione dei flussi illeciti nonché la ricostruzione dei circuiti di frode e delle connesse responsabilità.

In tali contesti, i principali reati tributari accertati di cui al d.lgs. n. 74/2000 sono quelli previsti dagli artt. 2 (Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti), 5 (Omessa dichiarazione), 8 (Emissione di fatture o altri documenti per operazioni inesistenti) e 10 (Occultamento o distruzione di documenti contabili).

Le fatture per operazioni inesistenti possono essere utilizzate non solo per evadere le imposte, ma anche per dissimulare i traffici illeciti di rifiuti. In questo caso, nelle fatture e nei documenti di trasporto tali beni vengono dichiarati come altri prodotti non soggetti alle disposizioni concernenti gli obblighi sulla circolazione dei rifiuti.

Ad esempio, attraverso fatture attestanti falsamente la cessione intracomunitaria di rifiuti o rottami metallici a società cartiere estere, le organizzazioni criminali documentano la fuoriuscita dal territorio nazionale dei prodotti in argomento, che vengono, invece, riversati in discariche abusive o ceduti "in nero" ad altre imprese per il relativo trattamento.

Con specifico riferimento al regime fiscale di settore, al fine di evitare che le attività illecite connesse al ciclo di rifiuti comportino anche una perdita di gettito per l'Erario in termini di IVA, l'art. 74, settimo comma, del D.P.R. n. 633/1972 prevede che «*Per le cessioni di rottami, cascami e avanzi di metalli ferrosi e dei relativi lavori, di carta da macero, di stracci e di scarti di ossa, di pelli, di vetri, di gomma e plastica, nonché di bancali in legno (pallet) recuperati ai cicli di utilizzo successivi al primo, intendendosi comprese anche quelle relative agli anzidetti beni che siano stati ripuliti, selezionati, tagliati, compattati, lingottati o sottoposti ad altri trattamenti atti a facilitarne l'utilizzazione, il trasporto e lo stoccaggio senza modificarne la natura, al pagamento dell'imposta è tenuto il cessionario, se soggetto passivo d'imposta nel territorio dello Stato*».

Pertanto, per le cessioni in argomento, il cedente emetta fattura senza addebitare l'IVA, essendo posto a carico del cessionario l'obbligo di integrare la fattura con la relativa imposta secondo il meccanismo dell'inversione contabile (c.d. *reverse charge*). Le cessioni che rilevano ai fini di tale disposizione, come chiarito dall'Agenzia delle entrate (cfr. circolare n. 43/E del 12 maggio 2008), sono afferenti sia ai rottami "nuovi" (ossia gli scarti di lavorazione) sia a quelli "vecchi", provenienti, ad esempio, dalla raccolta dei rifiuti.

Scontano l'aliquota IVA ridotta del 10%, invece, le principali prestazioni di servizio connesse al ciclo dei rifiuti, indicate nel punto n. 127-*sexiesdecies* della Tabella A, Parte III, allegata al D.P.R. n. 633/1972;

(ii) **corruzione e falsità nei provvedimenti autorizzativi**.

Il traffico illecito dei rifiuti viene spesso gestito ed organizzato da imprese che non dispongono dei requisiti previsti dalla normativa di settore per il trattamento dei rifiuti, ma appaiono formalmente idonee a svolgere tale attività in virtù di provvedimenti autorizzatori rilasciati dagli enti preposti dietro compiacenti atteggiamenti corruttivi dei funzionari.

Tale *modus operandi* ha quale immediata conseguenza quella di alterare il libero mercato, con l'ineluttabile estromissione delle aziende lecite che, nell'osservare le prescrizioni normative, sono gravate da numerosi oneri di gestione e quindi costrette a praticare prezzi meno competitivi delle imprese infiltrate.

I.A. nei reati economici e finanziari

di Gaetano Ruta, Sostituto Procuratore Tribunale di Milano

SOMMARIO: 1. Premessa. – 2. L'uso dell'Intelligenza Artificiale nei mercati finanziari: analisi di contesto. – 2.1. In particolare: il sistema di *High Frequency Trading*. – 2.2. Le negoziazioni attraverso social media e piattaforme online non regolamentate. – 2.3. Consulenza *online* e *robo advisor*. – 3. Descrizione dell'utilizzo dell'Intelligenza Artificiale per commettere condotte di manipolazione del mercato. – 4. Alcuni casi giudiziari. – 4.1. Caso *Da Vinci Invest Limited.* – 4.2. Caso *Paul Axel Walter.* – 4.3. Caso *Michael Coscia*. – 5. Il quadro regolamentare. – 6. La prospettiva dei penalisti.

1. Premessa.

L'applicazione dell'Intelligenza Artificiale nei mercati finanziari costituisce da tempo materia di riflessione in diversi ambiti del sapere, da quello tecnologico a quello economico e giuridico. I mercati finanziari si prestano ad una profonda capacità di innovazione ed i sistemi di intelligenza artificiale hanno trovato in questo campo un fertile terreno di penetrazione.

La riflessione interna al gruppo di lavoro ha tratto beneficio dalle competenze che, in ciascun ambito, i soggetti coinvolti – Cassa Depositi e Prestiti, Consob, Guardia di Finanza e Magistratura – hanno sviluppato.

Si parte da un comune dato di realtà: l'Intelligenza Artificiale – almeno entro lo spettro dei mercati finanziari – non rappresenta una prospettiva futura: è il presente. Si può anzi aggiungere che questo fenomeno ha maturato una propria storia, mettendo a nudo limiti e potenzialità ed interrogando operatori, regolatori ed organi di controllo sul governo degli strumenti tecnologici che ne sono a fondamento.

È evidente l'influsso, se non sul piano giuridico certamente su quello empirico, proveniente dal mondo anglosassone, in particolare dagli Stati Uniti. Le risposte regolamentari possono non coincidere, è un fatto tuttavia che l'operatività dei sistemi di intelligenza artificiale nel campo dei mercati finanziari, con l'individuazione di limiti e problemi, parte proprio dagli Stati Uniti, ove hanno avuto incubazione e sviluppo tutti i processi tecnologici avanzati.

Il lavoro si articola quindi su una ricognizione dei nodi applicativi sinora emersi e sulle risposte regolamentari che sono state date. Chiuderà il testo una riflessione, fondata sugli studi della dottrina che in Italia ha affrontato questi temi, rispetto alle implicazioni nel diritto penale.

2. L'uso dell'Intelligenza Artificiale nei mercati finanziari: analisi di contesto.

Con il termine *Fintech* (Finanza Tecnologica) si intende in modo generico la tecnologia applicata alla finanza. Poiché tale termine non assume contorni operativi ben delimitati, pare più corretto riferirsi ad un "ampio insieme di innovazioni – osservabili in campo finanziario in senso lato – che sono rese possibili dall'impiego delle nuove tecnologie sia nell'offerta di servizi agli utenti finali sia nei «processi produttivi» interni agli operatori finanziari nonché nel disegno di imprese-mercato (il c.d. *financial marketplace*)"[58]. Le potenzialità offerte dalle nuove tecnologie risultano, dunque, particolarmente sviluppate nel settore dei mercati finanziari posto che consentono di offrire nuove tipologie di servizi, prodotti, modelli di business (o di modificarne le modalità di offerta) grazie alla possibilità di effettuare milioni di operazioni al secondo, con una conseguente significativa riduzione dei costi, un aumento dei profitti e un'ottimizzazione dei prodotti, senza incorrere in errori o *bias* umano. A fronte di queste opportunità emerge il rischio concreto che le innovazioni tecnologiche possano essere strumento diretto o indiretto attraverso il quale commettere condotte illecite, ovvero vittime delle condotte stesse[59].

Al centro di questo sistema si colloca la costruzione di algoritmi, pensati e realizzati per sostituire sempre di più il ruolo dell'essere umano.

Nel settore dei mercati finanziari è possibile individuare quattro ambiti applicativi di maggior rilievo: la negoziazione ad alta frequenza o *HFT – High Frequency Trading (Negotiation)*, le negoziazioni attraverso *social media* e piattaforme *online* non regolamentate, la consulenza finanziaria automatizzata e la valutazione del merito creditizio.

Particolare rilevanza, ai fini che qui interessano, va accordata ai sistemi di negoziazione ad alta frequenza: gli algoritmi sono utilizzati per realizzare un numero elevato di negoziazioni in un arco temporale ristrettissimo, realizzando profitti tramite arbitraggi tra diversi mercati o l'intervallo tra ordine ed esecuzione. Per un maggiore approfondimento concettuale si rimanda al paragrafo che segue: studi elaborati dall'ESMA evidenziano come a partire soprattutto dal 2018 l'incremento del *trading* algoritmico, con riferimento al mercato azionario europeo (inferiore, per il vero, l'incidenza sul mercato obbligazionario e dei derivati), sia del 50-70%[60]. Con riferimento al contesto nazionale, gli scambi riconducibili agli High frequency traders nel Mercato Telematico Azionario (MTA) si sono attestati nel periodo 2016 – 2019 intorno al 30% del

---

[58] Cfr. C. SCHENA – A. TANDA – C. ARLOTTA – G. POTENZA, "Lo sviluppo del FinTech", Quaderni FinTech, Consob, 1/2018, https://www.consob.it/documents/46180/46181/FinTech_1.pdf/35712ee6-1ae5-4fbc-b4ca-e45b7bf80963#page=15.

[59] Cfr. V. CARLINI, "Il lato oscuro dei listini: così gli algoritmi manipolano i mercati", Il Sole 24 Ore, 29 aprile 2018, https://www.ilsole24ore.com/art/il-lato-oscuro-listini-cosi-algoritmi-manipolano-mercati-AE1qK3eE.

[60] Cfr. ESMA – European Securities and Markets Authority "Consultation Paper. MiFID II/MiFIR review report on Algorithmic Trading", 18 dicembre 2020, https://www.esma.europa.eu/sites/default/files/library/esma-70-156-2368_mifid_ii_consultation_paper_on_algorithmic_trading.pdf, pag. 21.

totale degli scambi conclusi, con una contrazione nell'ultimo anno di riferimento al 26%[61].

Un impatto significativo hanno le negoziazioni attraverso *social media* e piattaforme non regolamentate, che attraverso un meccanismo diffusivo esponenziale possono produrre rilevanti effetti distorsivi.

Il terzo ambito è relativo alla consulenza finanziaria automatizzata, nota come *robo advice*, per cui algoritmi rilasciano raccomandazioni di investimenti in strumenti finanziari, che sono presentate come adatte ad un determinato cliente. Con riferimento a tale fattispecie emerge la necessità di realizzare una profilazione dell'utenza[62].

La quarta area concerne la valutazione del merito creditizio, ossia la possibilità di concedere un determinato prestito, effettuata da un algoritmo sulla base delle informazioni raccolte.

2.1. In particolare: il sistema di High Frequency Trading.

Uno degli eventi che ha maggiormente attratto l'attenzione del pubblico sull'influenza della tecnologia nei mercati finanziari è stato il cosiddetto *Flash Crash* avvenuto negli Stati Uniti d'America nel 2010. Più precisamente, il 6 maggio 2010, in un contesto di mercato al ribasso, intorno alle 14:40, in pochi minuti di scambi l'indice Dow Jones perse quasi 1.000 punti, recuperando nei successivi minuti, quasi 600 punti.

In quell'occasione raggiunse la ribalta mediatica un nuovo modello di operatività nonché nuove strategie di negoziazione che rapidamente stavano acquistando spazi nei mercati finanziari mondiali e che condusse quell'anno stesso la *U.S. Securities & Exchange Commission* (SEC), la U.S. *Commodity Futures Trading Commission* (CFTC) nonché il Parlamento Europeo a investigare il fenomeno[63], che adesso viene ricondotto pacificamente nella definizione di "negoziazione ad alta frequenza" (HFT- *High-Frequency Trading*).

Si tratta dei cd. algoritmi di decisione sugli investimenti che prendono decisioni automatizzate di negoziazione stabilendo quali strumenti finanziari acquistare o vendere con intervento umano minimo o nullo, nonché dei cd. algoritmi di esecuzione degli ordini, che ottimizzano il processo di esecuzione degli ordini mediante la

---

[61] Cfr. CONSOB – Commissione Nazionale per le Società e la Borsa, "Relazione per l'anno 2019", 31 marzo 2020, https://www.consob.it/documents/46180/46181/rel2019.pdf/12ba0788-ec9b-4c53-80fs-e91c6a5de98a.

[62] Per approfondimenti sul tema si veda M. CARATELLI – C. GIANNOTTI – N. LINCIANO – P. SOCCORSO, "Valore della consulenza finanziaria e *robo advice* nella percezione degli investitori" Quaderni FinTech, Consob, 6/2019, https://www.consob.it/documents/46180/46181/FinTech_6.pdf/185b1db5-d48f-4bd9-864b-082e356cb992.

[63] Il riferimento è fatto al documento "*Findings regarding the market events of may 6, 2010 – Report of the staffs of the CFTC and SEC to the joint advisory committee on emerging regulatory issues – September 30, 2010*", ora disponibile all'indirizzo https://www.sec.gov/files/marketevents-report.pdf; nonché alla "*Relazione sulla regolamentazione della negoziazione di strumenti finanziari, di Kay Swinburne – 16.11.2010 (2010/2075(INI)"* che può leggersi all'indirizzo https://www.europarl.europa.eu/doceo/document/A-7-2010-0326_IT.pdf.

generazione e la trasmissione automatizzate degli ordini o delle quotazioni ad una o più sedi di negoziazione, una volta che la decisione di investimento è stata presa.

L'utilizzo di questa nuova tecnologia di negoziazione ha aumentato la velocità, la capacità e la complessità delle modalità di negoziazione degli investitori. Essa ha inoltre consentito ai partecipanti ai mercati finanziari di facilitare l'accesso elettronico diretto ai mercati per i loro clienti mediante l'utilizzo dei loro sistemi di negoziazione, il cd. accesso diretto ai mercati o il cd. accesso sponsorizzato.

Tale tecnologia è tuttavia all'origine anche di una serie di rischi potenziali, come un aumento del rischio di sovraccarico dei sistemi nelle sedi di negoziazione a causa del gran numero di ordini, ma soprattutto il rischio che la negoziazione algoritmica generi ordini erronei o doppi o che comunque non funzioni correttamente e crei così un mercato disordinato. Oltre al rischio che i sistemi di negoziazione algoritmica reagiscano in modo eccessivo ad altri eventi di mercato e possano manifestarsi fenomeni di manipolazioni del mercato.

2.2. Le negoziazioni attraverso social media e piattaforme online non regolamentate.

Un fenomeno passibile di rilevanti effetti distorsivi è rappresentato dalle operazioni di mercato sollecitate o comunque veicolate attraverso *social media* e altre piattaforme *online* non regolamentate. Occorre infatti evidenziare come episodi recenti, che hanno raggiunto l'apice alla fine di gennaio 2021, abbiano mostrato una volatilità molto elevata in alcuni titoli statunitensi, legata a un significativo accumulo di posizioni nette corte e all'azione concertata di alcuni investitori al dettaglio, sulla base delle informazioni condivise sui *social media*[64].

Un fenomeno di mercato nel quale un ruolo determinante nella vicenda è stato svolto dalle cd. "piattaforme di *trading*"[65] accessibili tramite semplici applicazioni, cd. *app*, dedicate ai dispositivi di tipo mobile, quali *smartphone* o *tablet*, che hanno reso più

[64] Ancora una volta la tecnologia in rapida evoluzione, e l'intersezione della stessa con i mercati dei capitali, ha mostrato potenzialità non prima considerate che si sono manifestate nei cd *forum online*, luoghi ove si incontrano vere e proprie comunità di individui, per discutere *online* di una varietà di argomenti in modo anonimo, inclusi la materia degli investimenti. Il *Forum* interessato nelle vicende di gennaio 2021 contava, all'epoca, circa 10 milioni di membri.

[65] Il termine "piattaforma di *trading*" non deve essere confuso alla nozione di "sede di negoziazione" come declinata, per quanto di interesse, nella normativa europea MiFID II. Non si tratta né di un sistema multilaterale di negoziazione – MTF, né di sistema organizzato di negoziazione – OTF, né tantomeno di mercati regolamentati. Si tratta, appunto di applicazioni utilizzate nell'interazione con la clientela da *broker/dealer* autorizzati, che consentono ai *broker* di veicolare il flusso di ordini verso le sedi di negoziazione e/o le controparti, attraverso algoritmi che verificano le condizioni migliori per la successiva esecuzione. Sistemi che, qualora siano limitati al solo reindirizzamento del flusso di ordini senza alcun ulteriore intervento sulla definizione dei parametri dell'ordine, non ricadono nella disciplina di attività di negoziazione algoritmica contenuta nella MiFID II e pertanto sono estranei dall'ambito di applicazione dei presidi previsti dalla stessa normativa Per quanto di interesse, in questa sede, si rappresenta che gli ordini vengono infatti trasmessi, tramite il cd. *order routing*, ad operatori ad alta frequenza che riconoscono al *broke*r somme variabili in funzione della dimensione del flusso di ordini.

facile per clienti al dettaglio iniziare a fare investimenti e ottenere consigli su come investire.

Per tale motivo, alla luce di questi recenti episodi (accaduti principalmente nel mercato statunitense), l'ESMA ha recentemente pubblicato una dichiarazione con la quale esorta gli investitori a prestare attenzione quando le decisioni di investimento sono basate esclusivamente su informazioni provenienti da *social media* e altre piattaforme *online* non regolamentate, se non sono in grado di verificarne l'affidabilità e la qualità[66]. L'Autorità europea rimarca, inoltre, come la diffusione tramite *social media* di informazioni false o fuorvianti su un emittente o uno strumento finanziario possa costituire una condotta rilevante ai fini della manipolazione del mercato.

È in questo contesto che si è inserito il tema del cd. "pagamento per il flusso degli ordini", *payment for order flow* (PFOF): la pratica delle imprese (*broker*) di ricevere pagamenti da sedi di esecuzione per dirigere il flusso degli ordini verso queste ultime[67].

Secondo quanto rilevato dalle Autorità di Vigilanza, il pagamento per il flusso degli ordini sembra essere stato un fattore importante per l'aumento dell'attività dei clienti al dettaglio osservato negli Stati Uniti. Esso pare avere avuto, ad esempio, un ruolo determinate nell'ambito delle vicende del gennaio 2021[68].

Pur essendo meno diffuso che negli Stati Uniti, il pagamento per il flusso degli ordini è stato osservato anche nell'Unione Europa[69]. La pratica del pagamento per il

---

[66] Cfr. ESMA, Statement, 17 febbraio 2021, https://www.esma.europa.eu/sites/default/files/library/esma70-155-11809_episodes_of_very_high_volatility_in_trading_of_certain_stocks_0.pdf.

[67] In proposito, si veda la "*Dichiarazione sui casi di anomala volatilità nella negoziazione di azioni e nell'utilizzo di social forum e piattaforme di trading online*" resa dalla Consob che può leggersi all'indirizzo https://www.consob.it/documents/46180/46181/dichiarazione_20210413.pdf/008ec336-5bb9-4e63-b66a-8780b2995637.

[68] Sul punto, il Sig. Gary Gensler, Presidente della *U.S. Securities and Exchange Commission* – SEC, ha precisato che la piattaforma di *trading* coinvolta nella vicenda ha ammesso pubblicamente di aver ottenuto 331 milioni di dollari in pagamenti per i ricavi da flusso degli ordini nel primo trimestre di quest'anno, più del triplo dell'importo che aveva riportato nel primo trimestre del 2020. Il Sig. Gary Gensler ha aggiunto che "*A differenza degli scambi pubblici che devono offrire un accesso equo alle loro quotazioni pubblicamente visualizzate, questi grossisti possono decidere se eseguire questi ordini direttamente o passarli per essere eseguiti dalle borse o altre sedi di negoziazione. Inoltre, i grossisti ottengono informazioni preziose da questo flusso di ordini che gli altri partecipanti al mercato ottengono con un ritardo, o non ottengono affatto. In molti aspetti dell'economia, dai social media ai motori di ricerca, l'accesso ai dati è un crescente vantaggio competitivo. I nostri mercati dei capitali non sono diversi. Volumi più elevati di operazioni generano più pagamenti per il flusso degli ordini. Questo fa venire in mente una serie di domande: i broker-dealer hanno conflitti di interesse intrinseci? In tal caso, i clienti ottengono la migliore esecuzione nel contesto di quel conflitto? I broker-dealer sono incentivati a incoraggiare i clienti a negoziare più frequentemente di quanto non sia nel migliore interesse di quei clienti? Quali sono le politiche? implicazioni rispetto ai dati aggregati dagli acquirenti del flusso degli ordini?*". Il testo dell'audizione del Presidente della SEC dinanzi alla Commissione per i servizi finanziari del Congresso degli Stati Uniti, svoltasi il 6 maggio 2021, è reperibile all'indirizzo https://financialservices.house.gov/uploadedfiles/hhrg-117-ba00-wstate-genslerg-20210506.pdf.

[69] Recenti iniziative sono state intraprese anche dall'Autorità europea degli strumenti finanziari e dei mercati – ESMA, si veda in argomento la dichiarazione disponibile all'indirizzo https://www.esma.europa.eu/press-news/esma-news/esma-newsletter-n%C2%BA21.
In proposito, l'ESMA ha rilevato come "*L'uso delle nuove tecnologie può contribuire ad aumentare la partecipazione degli investitori al dettaglio ai mercati finanziari, contribuendo così a uno degli obiettivi del piano*

flusso degli ordini solleva questioni in materia di protezione degli investitori, con particolare riferimento al rispetto delle disposizioni della MiFID 2 e dei relativi atti delegati.

In una recente dichiarazione pubblica[70] in merito al fenomeno del pagamento per il flusso degli ordini (*payment for order flow* – PFOF) l'ESMA ha evidenziato che la pratica della ricezione di pagamento per il flusso degli ordini (PFOF) coinvolge una serie di obblighi disciplinati dalla MiFID II volti a garantire che le imprese di investimento agiscano nel migliore interesse dei loro clienti durante l'esecuzione dei loro ordini e, più precisamente, la *best execution*[71], il regime di incentivi e la trasparenza dei costi. In proposito, l'ESMA ha dichiarato che i "*PFOF sollevano seri problemi di protezione degli investitori* […] *e alla luce di tali preoccupazioni e dei molteplici requisiti applicabili alla PFOF, l'ESMA ritiene che nella maggior parte dei casi sia improbabile che la PFOF possa essere compatibile con la direttiva MiFID II e i suoi atti delegati*".

Deve evidenziarsi infatti che la ricezione di pagamenti per il flusso degli ordini da parte di terzi provoca per l'impresa che esegue gli ordini dei clienti un chiaro conflitto di interessi con i propri clienti, in quanto la stessa è incentivata a scegliere il soggetto che offre il pagamento più elevato, piuttosto che il miglior risultato possibile per i suoi

---

d'azione per l'Unione dei mercati dei capitali. Tuttavia, si teme che aspetti specifici dei modelli di business dei broker online possano incentivare l'adozione di strategie di trading rischiose a breve termine da parte degli investitori al dettaglio. Inoltre, vi sono potenziali preoccupazioni circa la trasparenza della struttura delle commissioni. In particolare, dovrebbe essere ulteriormente studiato il ruolo dei modelli di business dei broker online nel creare la recente impennata della partecipazione degli investitori al dettaglio".

[70] La dichiarazione pubblica è disponibile all'indirizzo https://www.esma.europa.eu/sites/default/files/library/esma35-43-2749_esma_public_statement_pfof_and_zero-commission_brokers.pdf . Più nello specifico, il riferimento è ai presidi relativi 1) all'adozione di tutte le misure sufficienti per ottenere il miglior risultato possibile per i loro clienti (*best execution*), 2) ai conflitti di interesse, 3) agli incentivi e 4) alla trasparenza dei costi. La ricezione del pagamento per il flusso degli ordini da terze parti (*market makers*) potrebbe determinare un conflitto di interessi tra l'impresa (*broker*) e i suoi clienti, incentivando l'impresa a scegliere la terza parte che offre il pagamento più alto invece del miglior risultato possibile per i suoi clienti. Quanto ai conflitti di interessi e alla *best execution*, si evidenzia che la MiFID 2 obbliga le imprese ad adottare tutte le misure appropriate per identificare e prevenire o gestire i conflitti di interessi. Conseguentemente, la scelta di un terzo per l'esecuzione degli ordini dei clienti dovrebbe essere guidata esclusivamente dall'obiettivo di ottenere il miglior risultato possibile per i clienti e non dovrebbe in alcun modo essere influenzata dalla quantità di pagamento per il flusso degli ordini che il terzo è disposto a corrispondere all'impresa. A tal fine, gli accordi di esecuzione di un'impresa dovrebbero considerare sia le terze parti disposte a fornire pagamento per il flusso degli ordini che quelle non disposte a fornire pagamento per il flusso degli ordini, e i fattori utilizzati per scegliere una terza parte rispetto ad un'altra dovrebbero essere strettamente correlati all'ottenimento del miglior risultato per il cliente (che per i clienti al dettaglio – in assenza di specifiche istruzioni – deve essere valutato globalmente, avuto riguardo al prezzo ed ai costi). A tale fine le imprese devono prestare particolare attenzione al rischio che la ricezione di pagamenti per il flusso degli ordini da terzi possa influenzare lo *spread* denaro-lettera offerto da tali terzi, determinando un prezzo peggiore per il cliente rispetto alla situazione in cui il terzo non corrisponde il pagamento per il flusso degli ordini.

[71] L'obbligo di ottenere la migliore esecuzione (cd *best execution*), ora previsto dall'art.7, paragrafo 1, della direttiva Mifid e declinato nell'art. 64 del Regolamento delegato 2017/565, stabilisce che un'impresa di investimento deve adottare tutte le misure sufficienti per ottenere il miglior risultato possibile per il proprio cliente quando esegue un ordine del cliente.

clienti. Non può escludersi, infatti, che il pagamento per il flusso degli ordini costituisca un incentivo ricevuto da terzi in relazione al servizio di investimento fornito al cliente.

Sempre in questa prospettiva, l'ESMA sottolinea che le imprese dovrebbero considerare il pagamento per il flusso degli ordini come un costo per i clienti[72]. Le imprese che ricevono il pagamento per il flusso degli ordini da terzi dovrebbero quindi fornire informazioni su tutti i costi e gli oneri a carico del cliente relativi al servizio e agli strumenti, comprese, tra l'altro, le informazioni sui costi impliciti (ad esempio quelli inclusi nello *spread bid-ask)*.

La pratica del pagamento per il flusso di ordini presenta poi aspetti di particolare attenzione da parte delle Autorità di vigilanza allorquando le imprese eseguono gli ordini dei clienti e commercializzano i loro servizi precisando che non comportano costi per gli investitori. In alcuni casi, l'assenza di commissioni esplicite per l'esecuzione degli ordini dei clienti è prevista solo per alcuni degli strumenti finanziari offerti. Si tratta dei cd. "*broker a commissione zero*" che spesso ricevono pagamenti per il flusso degli ordini PFOF da terze parti, circostanza questa che potrebbe per l'impresa compensare la mancanza di commissioni dirette addebitate ai clienti per l'esecuzione degli ordini.

Tale caratteristica dei cd. "*broker a commissione zero*" si è trovata collegata al fenomeno descritto come *order routing* che consente ad operatori ad alta frequenza di riconoscere al *broker* somme variabili in funzione della dimensione del flusso di ordini. Allo stato, si tratta di un fenomeno che ha interessato gli Stati Uniti ed è emerso con evidenza nell'ambito della vicenda Gamestop del gennaio 2021[73].

L'Autorità europea ha concluso la dichiarazione con la richiesta rivolta alle Autorità di vigilanza nazionali di "*dare priorità alla PFOF nelle loro attività di vigilanza per il 2021 o l'inizio del 2022, in particolare negli Stati membri in cui è stata osservata la PFOF. Tali attività di vigilanza dovrebbero mirare a valutare l'impatto effettivo del PFOF sul rispetto da parte delle imprese dei requisiti in materia di esecuzione alle migliori prestazioni, conflitti di interesse e incentivi, anche se le imprese che ricevono PFOF sono in grado di dimostrare di aver costantemente conseguito il miglior risultato possibile per i clienti al dettaglio nell'esecuzione dei loro ordini, tenendo conto, se del caso, delle attività transfrontaliere delle imprese*".

---

[72] Alla luce della disciplina MiFID 2 in materia di incentivi, le imprese che ricevono pagamento per il flusso degli ordini devono rivelare chiaramente l'esistenza, la natura e l'importo del pagamento per il flusso degli ordini al cliente sia *ex-ante* che *ex-post*.

[73] Nella audizione dinanzi alla Commissione per i servizi finanziari del Congresso degli Stati Uniti in merito alle vicende del gennaio 2021, svoltasi il 6 maggio 2021, il Presidente della SEC ha dichiarato che "*alcune società commerciali cercavano di attirare il flusso di ordini di Robinhood* […] *e Robinhood ha offerto esplicitamente di accettare un minor miglioramento del prezzo per i suoi clienti in cambio di ricevere un pagamento più elevato per il flusso degli ordini che tale operatività aveva generato. Di conseguenza, molti clienti di Robinhood avrebbero così ritenuto di sostenere costi di esecuzioni inferiori; ma in realtà questi costi sono risultati superiori rispetto al risparmio che pensavano di ottenere dall'applicazione delle commissioni zero*".

2.3. Consulenza online *e* robo advisor.

Il tema dell'impatto di *social media* e piattaforme non regolamentate nello svolgimento di operazioni di *trading* è strettamente collegato alla realizzazione di consulenze *online*, idonee ad incidere sulla determinazione degli investitori potenzialmente al di fuori di ogni controllo.

In questa prospettiva, va segnalato come nello scorso mese di agosto la SEC ha lanciato una pubblica richiesta di informazioni in merito all'utilizzo delle piattaforme digitali per gli investimenti, ai cd. *broker online* e ai *robo-advisor* [74]. Nello specifico, la Securities and Exchange Commission ha richiesto informazioni e commenti pubblici su questioni relative a: *broker-dealer* e consulenti per gli investimenti, utilizzo di "*pratiche di coinvolgimento digitale*" o "DEP", inclusi suggerimenti comportamentali, marketing differenziale, funzionalità simili a giochi (comunemente denominate "*gamification*") e altri elementi di progettazione o funzionalità per interagire con gli investitori al dettaglio su piattaforme digitali (ad esempio, siti web, portali e applicazioni o "app"), nonché gli strumenti e i metodi analitici e tecnologici utilizzati in relazione a tali pratiche di coinvolgimento digitale; nonché, appunto, sull'uso della tecnologia da parte di un consulente per gli investimenti per sviluppare e fornire consulenza in materia di investimenti.

3. Descrizione dell'utilizzo dell'Intelligenza Artificiale per commettere condotte di manipolazione del mercato.

L'utilizzo delle nuove tecnologie nel settore dei mercati finanziari può prestarsi alla commissione di diversi illeciti penalmente rilevanti, quali la frode informatica, il riciclaggio e il finanziamento del terrorismo, l'abusivismo finanziario e le condotte di manipolazione del mercato.

Con riferimento a queste ultime, l'utilizzo di algoritmi, da un lato, ha agevolato l'esecuzione di tecniche manipolative comuni, dall'altro, ha consentito l'ideazione di nuove forme che richiedono necessariamente l'impiego di HFT. In entrambe le ipotesi l'uso delle nuove tecnologie è in grado di amplificare gli effetti negativi per il mercato.

Si possono individuare le seguenti tecniche:

(1) "***Momentum ignition***", evoluzione della tecnica del c.d. *pump and dump*. Un operatore, dopo aver individuato un titolo dal prezzo tendenzialmente stabile, assume, sulla base di una analisi automatizzata di tutti i dati di mercato, una posizione aggressiva, aumentando improvvisamente i volumi di scambio su quello strumento. L'effetto prodotto sarà una forte oscillazione del prezzo, che permetterà all'algoritmo di chiudere la propria posizione attraverso un'operazione di segno opposto a quelle iniziali, a prezzi prima non disponibili.

[74] Il testo è reperibile all'indirizzo https://www.sec.gov/rules/other/2021/34-92766.pdf.

(2) "***Quote stuffing***", che consiste nell'immissione e contestuale cancellazione di un numero elevato di ordini in grado di generare fenomeni di congestione dei sistemi operativi e compromettere l'accesso al mercato da parte degli altri operatori comuni. Tale circostanza può consentire al *trader* di trarre vantaggio, ad esempio, dai cosiddetti 'arbitraggi da latenza', ossia dalle divergenze di prezzo per un medesimo titolo che non hanno altra causa se non le temporanee (di durata infinitesimale) inefficienze operative di carattere informatico nei sistemi di accoppiamento automatico tra domanda ed offerta.

(3) "***Smoking***", che implica l'avanzamento da parte di un operatore di ordini dalle condizioni particolarmente 'allettanti' sul mercato al fine di attrarre investitori, per poi modificarli rapidamente attraverso l'inserimento di condizioni meno favorevoli prima ancora che le controparti attratte nella transazione possano rendersi conto del mutato scenario.

(4) "***Spoofing***", noto anche come 'painting the tape', consiste nell'immettere una serie di ordini di vendita, normalmente con offerte superiori al miglior prezzo presente sul book, al fine di indurre gli altri investitori a credere che sia cominciata una fase di ribasso del titolo stesso. L'algoritmo cancellerà tali ordini prima che siano eseguiti e, nel frattempo, immetterà un ordine di acquisto a prezzi che oramai saranno stati influenzati dalla pressione sul lato dell'offerta, traendo pertanto profitto a scapito degli altri investitori.

(5) "***Layering***" è una tecnica simile allo *spoofing* e consiste nell'immettere un ordine nascosto (non visibile nel book di negoziazione) in acquisto o vendita e un altro ordine palese visibile nel book dal lato opposto (vendita/acquisto) in modo da indurre gli altri operatori a credere che il mercato si stia muovendo verso un ribasso del prezzo e ad agire di conseguenza.

(6) "***Pinging***", attraverso questa tecnica, al pari delle ultime tre strategie descritte, l'operatore simula comportamenti ricorrenti, finalizzati a permettere al sistema di HFT di apprendere progressivamente lo schema di investimento di altri operatori e, poi, spingerli alla negoziazione fuorviati dal quadro di condizioni artatamente create dal sistema. In sostanza, l'HFT genera profitti solo ed esclusivamente grazie alle perdite dei traders tradizionali o algoritmici meno evoluti.

(7) "***Front running***". Si tratta di una modalità conseguente alla conoscenza di informazioni privilegiate relative a grossi ordini di acquisto o vendita in arrivo sul mercato. Sfruttando la velocità per immettere un ordine (*flash trade*) pochi istanti prima che venga immesso l'ordine in questione, il trader riesce a trarre profitto dalla transazione.

Alle citate forme di manipolazione si possono aggiungere quelle che prevedono l'intervento di altri operatori, come nel caso di c.d. "*Pre-arranged trading*", definito anche come "*improper matched orders*", o l'alterazione dei prezzi di strumenti su un mercato finalizzata allo scambio più vantaggioso degli stessi, derivante dall'aumento o diminuzione dei volumi di scambio anche su altre piattaforme – c.d. *market setting*.

Gli strumenti di intelligenza artificiale possono essere utilizzati per realizzare manipolazioni del mercato anche attraverso la diffusione di notizie false attraverso i *social media* in grado di influenzare la volatilità dei titoli. In particolare, attraverso i

«Bots» informazioni non veritiere su società quotate possono essere ripetute molteplici volte e influenzare il *sentiment* intorno l'azienda stessa o uno strumento finanziario. I nuovi algoritmi di intelligenza artificiale che operano sul mercato in modo automatico sono in grado di cogliere tali mutamenti, con il rischio di venire ingannati. I rischi di manipolazione informativa non sono meno gravi di quella operativa ed hanno sollecitato, come si è evidenziato sopra, interventi delle autorità di regolazione del mercato.

4. Alcuni casi giudiziari.

La casistica che segue fornisce una rappresentazione esemplificativa di alcuni casi di *market abuse* nei quali il meccanismo massivo di ordini, tipico della negoziazione nei HFT trova attuazione. Sono significativi i riferimenti temporali e locali: vicende avvenute nell'ultimo decennio, nelle giurisdizioni inglese ed americana. Sembrerebbe la conferma, sul piano empirico, di un fenomeno che ha già manifestato i primi effetti e richiesto una risposta sul piano regolatorio.

4.1. Caso Da Vinci Invest Limited.

Il caso in esame ha per oggetto un giudizio civile promosso davanti l'Alta Corte di Giustizia dalla FCA (*Financial Conduct Authority*[75]) nei confronti di un gruppo di società con a capo la Da Vinci Invest AG per manipolazione di mercato riconducibile alla tipologia del *Layering* o *Spoofing*.

I convenuti sono, tra gli altri i seguenti soggetti:

- Da Vinci Invest Ltd (di seguito, anche DVI), società inglese che operava da una filiale in Svizzera in qualità di gestore di fondi di investimento, sottoposta alla vigilanza dell'Autorità elvetica (FINMA);

- Da Vinci Invest Pte Limited (DVPte), società di Singapore;

- tre *traders,* cittadini ungheresi, ivi residenti all'epoca dei fatti contestati. Questi erano già stati coinvolti in operazioni manipolative, del tipo *layaring,* attraverso la Swift Trade Inc negli anni 2007 e 2008 e per questo successivamente sanzionata.

Come evidenziato la condotta di manipolazione contestata rientra nella categoria del *Layering* o *Spoofing*, in relazione alle quali il giudice fornisce le seguenti definizioni (peraltro, così appare dal tenore della motivazione, mutuate da precedenti casi)[76]: il *Layering* consiste nella pratica di inserire relativamente grandi ordini su un lato del *book* di scambio senza una genuina intenzione di dargli esecuzione: gli ordini vengono inseriti a prezzi che difficilmente sono in grado di attrarre controparti, almeno nelle intenzioni

[75] La *Financial Conduct Authority* è l'Autorità di vigilanza dei mercati finanziari del Regno Unito. La decisione può essere consultata al seguente link http://www.bailii.org/ew/cases/EWHC/Ch/2015/2401.html.

[76] "*The following general description of 'layering' or 'spoofing' offered by the FCA was accepted by the Upper Tribunal in 7722656 Canada Inc (t/a Swift Trade) v FSA [2013] Lloyd's LR (FC) 381 at paragraph 6*".

di chi li inserisce, ma che sono comunque idonei a determinare una variazione del prezzo dell'azione, come conseguenza dell'adeguamento provocato dal mercato per effetto di un apparente spostamento dell'equilibrio tra domanda e offerta. Al movimento consegue l'esecuzione di un'operazione sull'altro lato del libro degli ordini, con l'ottenimento di un profitto. Questo scambio è a sua volta seguito dalla cancellazione rapida dei grandi ordini che erano stati inseriti allo scopo di provocare il movimento del prezzo. L'operazione viene ripetuta più volte. Da tale descrizione si rileva come il termine *Layering* identifichi l'immissione di più ordini progettati per non essere scambiati su un lato del *book*, mentre *Spoofing* si riferisca al fatto che tale immissione crea una falsa impressione sulle vere intenzioni commerciali del *trader*. Nel caso specifico era accaduto quanto segue.

I *traders* della Swift Trade si accordarono nel 2010 con DVI, per impiegare il capitale disponibile in operazioni su derivati – c.d. CFD[77] – sul LSE – London Stock Exchange. Per accedere a tali negoziazioni si accordarono con Goldman Sachs per la fornitura di servizi DMA (*Direct Market Access*) e con la RealTick per la fornitura del *software* di collegamento con i citati servizi. In particolare, Goldman Sachs fornì tre sottoconti in nome di DVI, uno per ciascun *trader*.

I *traders* richiesero a Goldman Sachs di non utilizzare l'instradamento intelligente degli ordini[78] della società, in quanto la loro strategia sarebbe stata quella di negoziare separatamente nei diversi mercati (e con ciò, evidentemente, accrescere l'effetto dissimulatorio sotteso a queste operazioni). Il 21 dicembre 2010 la stessa Goldman Sachs inoltrò alla FSA una segnalazione di operazioni sospette per *market abuse*, in relazione ad operazioni condotte da DVI nel periodo agosto – dicembre dello stesso anno. Immediatamente dopo interruppe l'accesso tramite DMA.

Nel gennaio 2011, DVPte si accordò con SunGard, filiale inglese di una società americana, per attivare i servizi DMA, utilizzando sempre l'interfaccia di Realtick, e per la creazione di due sottoconti. Nel maggio del 2011, a seguito di altre segnalazioni da parte di alcuni operatori del mercato, l'Autorità di vigilanza avviò un'investigazione.

Operazioni, come si vede, protratte nel tempo e proseguite nonostante la presenza di segnali di allarme, grazie alla capacità dei *traders* di trovare società compiacenti e soluzioni per proseguire l'attività illecita.

Per quanto concerne il profilo della responsabilità degli enti, è interessante notare come l'attribuzione della responsabilità per manipolazione di mercato in capo ad una società venga ricondotta al solo elemento oggettivo, ricorrendo alle regole relative al contratto di agenzia. Questa soluzione risulta essere ancora più importante nel contesto in esame ossia della negoziazione sui mercati regolamentati. Frequentemente, il *trading*

---

[77] Un CFD è un tipo di investimento in derivati. Il caso in esame ha per oggetto CFD relativi ad azioni negoziate sulla LSE. Un CFD relativo ad azioni è un accordo in base al quale le parti condividono di pagare o ricevere la differenza di valore di una determinata azione tra l'ora e la data quando il contratto è aperto (stipulato) e l'ora e la data in cui il contratto è chiuso (terminato).

[78] L'instradamento intelligente degli orini consente che gli stessi vengono indirizzati alla borsa valori o MTF (*Multilateral Trading Facilities*) su cui si trova il miglior volume e/o prezzo visualizzato. In alternativa, l'investitore può richiedere che questa funzionalità sia disattivata in modo che possa controllare su quale piattaforma di *trading* viene inserito l'ordine.

viene effettuato con alti volumi e ad alta velocità da numerosi dipendenti di aziende che utilizzano complessi sistemi informatici. Il giudice ritiene che sarebbe contrario alla finalità perseguita dalla normativa in oggetto, se le società coinvolte potessero sottrarsi alla responsabilità per le azioni dei loro dipendenti, sostenendo che gli alti direttori o dirigenti della società non avessero effettivamente diretto il *trading* in questione o non sapessero ciò che veniva fatto sulle piattaforme di *trading* elettronico dai loro dipendenti o anche da programmi informatici progettati o gestiti dai loro dipendenti. Viene precisato che se si addivenisse ad un diverso parametro, la responsabilità per abuso di mercato potrebbe essere agevolmente evitata utilizzando il semplice espediente di coinvolgere *traders* che operano per suo conto come contraenti indipendenti piuttosto che come dipendenti. In sostanza, la natura del rapporto tra società e *trader*, sia esso come dipendente, appaltatore indipendente o joint venture, non dovrebbe fare alcuna differenza. Ciò che conta è se il comportamento in questione si verifica per conto della società.

In virtù di tale principio, viene ritenuta responsabile DVI per non aver vigilato sui *traders*, non avendo alcun rilievo che la relazione era legata alla partecipazione agli utili e non a un formale contratto di lavoro.

4.2. Caso Paul Axel Walter.

Il secondo caso ha per oggetto una sanzione irrogata nel 2017 dalla FCA nei confronti di un impiegato della *Bank of America Merrill Lynch International Limited* (BAML) per aver attuato nel 2014 una strategia che prevedeva l'inserimento di ordini che avevano quale obiettivo quello di indurre gli altri operatori del mercato che seguivano l'andamento dei titoli ad aumentare o a diminuire le quotazioni di modo da beneficiare di tale variazione del prezzo. In particolare, rappresentava al mercato l'intenzione di acquistare quando la sua volontà era quella di vendere e rappresentava l'intenzione di vendere quando la volontà era quella di comprare. Nel primo caso, le sue quotazioni fuorvianti, orientate verso la migliore offerta, hanno indotto gli altri operatori ad aumentare le loro offerte e viceversa.

Ciò che risulta particolarmente interessante è che la manipolazione è stata resa possibile sfruttando l'uso di algoritmi da parte degli altri operatori del mercato. Nello specifico, l'impiegato ha approfittato degli algoritmi in uso ad altri operatori che monitoravano le migliori offerte per attirarli verso le sue quotazioni e quindi negoziare poi a prezzi più alti o più bassi.

L'operatività dell'impiegato è stata denunciata da un altro operatore del mercato alla società che gestiva la piattaforma di *trading*[79].

[79] Il riferimento completo del caso si trova al seguente link: https://www.fca.org.uk/publication/final-notices/paul-axel-walter-2017.pdf.

4.3. Caso Michael Coscia.

Il terzo caso ha per oggetto la contestazione di una sanzione, nel 2013, nei confronti di un *trader* che ha operato per conto proprio attraverso il DMA adottando una tecnica manipolativa del tipo *Layering*. In particolare, piazzava e cancellava rapidamente ordini di grandi dimensioni che non intendeva negoziare nell'intento di creare una falsa impressione su acquirenti o venditori, "stratificando" il portafoglio ordini e così manipolando il mercato. Di particolare interesse, risulta esser in questo caso l'utilizzo di un programma algoritmico automatizzato progettato dall'operatore che operava contemporaneamente con due modalità.

La prima consisteva nel piazzare un piccolo ordine (in genere 10-20 lotti) sul libro degli ordini intorno al livello del miglior prezzo. Una volta che il piccolo ordine era in atto ("riposo"), diversi ordini grandi (oltre 50 lotti) venivano inseriti sull'altro lato del libro degli ordini.

I grandi ordini venivano immessi a livelli di prezzo in progressivo miglioramento. La sequenza di eventi veniva cronometrata per durare complessivamente circa 300 millisecondi, dopo i quali gli ordini (piccoli o grandi) venivano tutti annullati immediatamente e contemporaneamente, se non eseguiti in precedenza. Non appena l'ordine di acquisto piccolo veniva eseguito, il programma di *trading* annullava infatti, immediatamente e simultaneamente, tutti gli ordini di vendita di grandi dimensioni.

La seconda prevedeva l'utilizzo della stessa sequenza in senso inverso sul lato opposto del libro degli ordini in modo da negoziare la posizione creata con la prima modalità[80].

5. Il quadro regolamentare.

L'attività dei negoziatori algoritmici e dei negoziatori ad alta frequenza è entrata nel quadro regolamentare e di vigilanza della Consob attraverso la sottoposizione a regole stringenti e uniformi a livello europeo e all'introduzione di obblighi specifici sia per le imprese di investimento che si avvalgono delle suddette tecniche, sia per le sedi di negoziazione nell'ambito delle quali tali tecniche sono utilizzate.

La direttiva 2014/65/UE, cd. direttiva MiFID II e il regolamento delegato (UE) n. 2017/565 – quest'ultimo in materia di requisiti organizzativi e di condizioni all'esercizio dell'attività delle imprese di investimento – hanno fornito la definizione della negoziazione algoritmica[81] e della sottocategoria della negoziazione algoritmica ad alta

[80] Il riferimento completo del caso si trova al seguente link: https://www.justice.gov/usao-ndil/pr/high-frequency-trader-indicted-manipulating-commodities-futures-markets-first-federal.

[81] Ai sensi dell'articolo 4, paragrafo 1, punto 39, della direttiva 2014/65/UE, cd. MiFID II, la negoziazione algoritmica è definita come "*negoziazione di strumenti finanziari in cui un algoritmo informatizzato determina automaticamente i parametri individuali degli ordini, come ad esempio se avviare l'ordine, i tempi, il prezzo o la quantità dell'ordine o come gestire l'ordine dopo la sua presentazione, con intervento umano minimo o nullo e non*

frequenza[82] (HFT – *High Frequency Algorithmic Trading Technique*). Hanno stabilito inoltre che i soggetti ricadenti nella definizione di *negoziazione ad alta frequenza* debbano anche necessariamente essere autorizzati come impresa di investimento, anche qualora non svolgano nessun altro servizio o attività di investimento diverso dalla negoziazione in conto proprio[83].

In aggiunta, le imprese di investimento che utilizzano tecniche di negoziazione algoritmica sono sottoposte a specifici requisiti in termini di notifiche alle autorità competenti della propria attività, informazioni da fornire in merito agli ordini e alle operazioni riconducibili alla negoziazione algoritmica e ai presidi organizzativi volti a garantire il corretto svolgimento delle negoziazioni sul mercato. Analogamente, sono previsti numerosi obblighi a carico delle *sedi di negoziazione*, che consentano lo svolgimento di operatività algoritmica sulle proprie piattaforme di negoziazione[84].

L'attività degli HFT entra quindi nel quadro della vigilanza della Consob, da un lato, con riferimento alle informazioni trasmesse in merito all'attività svolta e all'obbligo di notifica all'Autorità dello svolgimento dell'attività su sedi di negoziazione e, dall'altro, relativamente ai presidi che i soggetti che svolgono tale attività devono

---

comprende i sistemi utilizzati unicamente per trasmettere ordini a una o più sedi di negoziazione, per trattare ordini che non comportano la determinazione di parametri di trading, per confermare ordini o per eseguire il trattamento post-negoziazione delle operazioni eseguite".

La definizione è ulteriormente specificata all'articolo 18 del regolamento delegato (UE) 2017/565, che stabilisce che "[...] *è considerato operare in assenza o con un limitato intervento umano se, per qualsiasi processo di ordine o di generazione della quotazione o per qualsiasi processo volto a ottimizzare l'esecuzione dell'ordine, un sistema automatizzato prende le decisioni in qualsiasi fase dell'inizializzazione, della generazione, della trasmissione o dell'esecuzione degli ordini o delle quotazioni in base a parametri predeterminati*".

[82] L'articolo 4, paragrafo 1, punto 40, della MiFID II definisce la tecnica di negoziazione algoritmica ad alta frequenza come "*qualsiasi tecnica di negoziazione algoritmica caratterizzata da: a) infrastrutture volte a ridurre al minimo le latenze di rete e di altro genere, compresa almeno una delle strutture per l'inserimento algoritmico dell'ordine: co-ubicazione, hosting di prossimità o accesso elettronico diretto a velocità elevata; b) determinazione da parte del sistema dell'inizializzazione, generazione, trasmissione o esecuzione dell'ordine senza intervento umano per il singolo ordine o negoziazione, e c) elevato traffico infragiornaliero di messaggi consistenti in ordini, quotazioni o cancellazioni*.

[83] L'esenzione dall'autorizzazione come impresa di investimento quando si negozia solo per conto proprio ai sensi dell'articolo 2, paragrafo 1, lettera d), della MiFID II non opera nel caso in cui un'impresa utilizza una tecnica di negoziazione algoritmica ad alta frequenza. L'autorizzazione richiesta mira a garantire che tali imprese siano soggette ai requisiti organizzativi previsti dalla MiFID II e che siano adeguatamente controllate. L'articolo 17, paragrafo 2, della MiFID II, stabilisce infatti che un'impresa di investimento che effettua negoziazione algoritmica notifica all'autorità nazionale competente del proprio Stato membro d'origine e della sede di negoziazione in cui l'impresa di investimento effettua la negoziazione algoritmica in qualità di membro o partecipante della sede di negoziazione.

[84] Un altro concetto importante nel contesto della tecnologia di negoziazione algoritmica è l'accesso elettronico diretto (DEA). Ai sensi dell'articolo 1, punto 41, della MiFID II, l'accesso elettronico diretto fa riferimento a "*un accordo in cui un membro o un partecipante o cliente di una sede di negoziazione consente a una persona di utilizzare il proprio codice di negoziazione in modo che la persona possa trasmettere elettronicamente ordini relativi a uno strumento finanziario direttamente alla sede di negoziazione e include accordi che comportano l'uso da parte di una persona dell'infrastruttura del membro o della persona o del cliente o di qualsiasi sistema di connessione fornito dal membro o partecipante o cliente, per trasmettere gli ordini (accesso diretto al mercato o DMA) e le disposizioni in cui tale infrastruttura non è utilizzata da una persona (accesso sponsorizzato)*".

predisporre ai sensi di quanto previsto dalla direttiva MiFID II e dal successivo regolamento delegato (UE) 2017/584[85].

In data 3 gennaio 2018 sono entrate in vigore le modifiche apportate al d.lgs. n. 58 del 1998 e successive modificazioni, cd. "TUF, *Testo unico delle disposizioni in materia di intermediazione finanziaria*", dal d.lgs. n. 129 del 3 agosto 2017, con cui sono state recepite nel nostro ordinamento la direttiva MiFID II e la Direttiva delegata (UE) 2017/593 e con cui è stata adeguata la normativa domestica al Regolamento (UE) n. 600/2014 (c.d. MiFIR).[86]

L'art. 2 della direttiva MiFID II ha trovato attuazione nell'art. 4-*terdecies* del d.lgs. n. 58 del 1998 che, allo scopo di incrementare la sicurezza e l'affidabilità delle transazioni che si svolgono sui mercati regolamentati (e sugli MTF), ha previsto la necessità che la negoziazione per conto proprio sia condizionata all'autorizzazione anche per le ipotesi in cui i "*negoziatori*" abbiano accesso elettronico diretto (DEA) a una sede di

---

[85] Il Regolamento delegato (UE) 2017/584 della Commissione, del 14 luglio 2016, che integra la direttiva 2014/65/UE del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per specificare i requisiti organizzativi delle sedi di negoziazione. Nel Regolamento è evidenziato che l'articolo 18, paragrafo 5, della direttiva 2014/65/UE, ha previsto che le disposizioni del Regolamento dovrebbero applicarsi non soltanto ai mercati regolamentati ma anche ai sistemi multilaterali di negoziazione e ai sistemi organizzati di negoziazione. L'impatto degli sviluppi tecnologici e in particolare della negoziazione algoritmica è uno dei fattori principali per determinare la capacità e i meccanismi di gestione delle sedi di negoziazione. I rischi derivanti dalla negoziazione algoritmica possono essere presenti in qualsiasi tipo di sistema di negoziazione supportato da mezzi elettronici. È pertanto opportuno stabilire requisiti organizzativi specifici per i mercati regolamentati, i sistemi multilaterali di negoziazione e i sistemi organizzati di negoziazione che consentono o autorizzano la negoziazione algoritmica mediante i loro sistemi. Tali sistemi di negoziazione sono quelli in cui può aver luogo la negoziazione algoritmica in contrapposizione a quelli in cui la negoziazione algoritmica non è permessa, compresi i sistemi di negoziazione in cui le operazioni sono disposte mediante negoziazione a voce (*voice negotiation*).

[86] La disciplina in materia di negoziazione algoritmica è anche contenuta nei provvedimenti legislativi di fonte europea di seguito indicati, adottati dalla Commissione su progetti di norme tecniche di regolamentazione (cd. *regulatory technical standards* – RTS) presentati alla Commissione da parte della Autorità di regolamentazione dei mercati mobiliari dell'Unione Europea (ESMA).

- Regolamento delegato (UE) 2017/587 della Commissione, del 14 luglio 2016, relativo agli obblighi di trasparenza per le sedi di negoziazione e le imprese di investimento in relazione ad azioni, certificati di deposito, fondi negoziati in borsa, certificati e altri strumenti finanziari analoghi e agli obblighi di esecuzione delle operazioni per talune azioni in una sede di negoziazione o da un internalizzatore sistematico;
- Regolamento delegato (UE) 2017/589 della Commissione, del 19 luglio 2016, relativo ai requisiti organizzativi delle imprese di investimento che praticano negoziazione algoritmica;
- Regolamento delegato (UE) 2017/578 della Commissione, del 13 giugno 2016, che integra la direttiva 2014/65/UE del Parlamento europeo e del Consiglio relativa ai mercati degli strumenti finanziari per quanto riguarda le norme tecniche di regolamentazione che specificano i requisiti relativi agli accordi e ai sistemi di market making;
- Regolamento delegato (UE) 2017/566 della Commissione, del 18 maggio 2016, che integra la direttiva 2014/65/UE del Parlamento europeo e del Consiglio relativa ai mercati degli strumenti finanziari per quanto riguarda le norme tecniche di regolamentazione per il rapporto tra ordini non eseguito e operazioni al fine di prevenire condizioni di negoziazione disordinate;
- Regolamento delegato (UE) 2017/588 della Commissione, del 14 luglio 2016, che integra la direttiva 2014/65/UE del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione relative al regime delle dimensioni dei *tick* per le azioni, i certificati di deposito e i fondi negoziati in borsa.

negoziazione ovvero nel caso in cui applichino una tecnica di negoziazione algoritmica ad alta frequenza.

Nel medesimo d.lgs. n. 58 del 1998 sono state inserite le definizioni di *negoziazione algoritmica* (art. 1, comma 6-*quinquies*), di *accesso elettronico diretto* (art. 1, comma 6-*sexies*), di *tecnica di negoziazione algoritmica ad alta frequenza* (art. 1, comma 6-*septies*). Ha trovato spazio, inoltre, la disciplina in merito ai *requisiti operativi delle sedi di negoziazione* (art. 65-*sexies*), alla *negoziazione algoritmica, accesso elettronico diretto, partecipazione a controparti centrali* (art. 67-*ter*), nonché l'attribuzione alla Consob della competenza per quanto riguarda la vigilanza sul rispetto dei requisiti da parte di Sim e banche italiane che svolgono negoziazione algoritmica [87].

La Consob ha esercitato la delega normativa di cui all'art. 67-*ter*, comma 8, e, operando le opportune modifiche al Regolamento Mercati, ha disciplinato i requisiti applicabili ai soggetti che effettuano negoziazione algoritmica e/o forniscono accesso elettronico diretto a una sede di negoziazione prevedendo *obblighi di registrazione* (art. 14), *comunicazioni in materia di negoziazione algoritmica* (art. 49), *comunicazioni in materia di accesso elettronico diretto* (art. 50).

In argomento, si segnala che l'ESMA ha pubblicato il 29 settembre 2021 il rapporto di revisione della MiFID II/MiFIR sulla negoziazione algoritmica[88]. Nel Rapporto Finale l'ESMA ha formulato alcune raccomandazioni che mirano sia a semplificare il regime sia a renderlo più efficiente e ha individuato le questioni che saranno seguite dall'ESMA tramite modifiche alle norme tecniche di regolamentazione e l'adozione di ulteriori orientamenti su una serie di argomenti. Detti argomenti includono: (*i*) i concetti di "*trading* algoritmico" e di "Accesso Elettronico Diretto"; (*ii*) il regime di autorizzazione per le società di negoziazione algoritmica dell'UE e non UE

---

[87] L'art. 67-*ter*, d.lgs. n. 58 del 1998, prevede che "*Le Sim e le banche italiane che svolgono negoziazione algoritmica: a) pongono in essere controlli dei sistemi e del rischio efficaci e idonei alla luce dell'attività esercitata sulle sedi di negoziazione, volti a garantire che i propri sistemi di negoziazione algoritmica siano resilienti e dispongano di sufficiente capacità, siano soggetti a soglie e limiti di negoziazione appropriati, impediscano di inviare ordini erronei o comunque recare pregiudizio all'ordinato svolgimento delle negoziazioni; b) pongono in essere controlli efficaci dei sistemi e del rischio per garantire che i sistemi di negoziazione algoritmica non possano essere utilizzati per finalità contrarie al regolamento (UE) n. 596/2014 o alle regole della sede di negoziazione; c) dispongono di meccanismi efficaci di continuità operativa per rimediare a malfunzionamenti dei sistemi di negoziazione algoritmica e provvedono affinché i loro sistemi siano soggetti a verifica e monitoraggio in modo adeguato per garantirne la conformità ai requisiti del presente comma.*

Le Sim e le banche italiane che effettuano negoziazioni algoritmiche lo notificano alla Consob e, se diversa, all'autorità competente dello Stato membro della sede di negoziazione in cui effettuano la negoziazione algoritmica quali membri o partecipanti o clienti della sede di negoziazione. La notifica è altresì effettuata alla Banca d'Italia per le sedi di negoziazione all'ingrosso di titoli di Stato […] *la Consob vigila sul rispetto dei requisiti previsti nel presente articolo da parte di Sim e banche italiane che svolgono negoziazione algoritmica. A tale fine la Consob può chiedere, su base regolare o ad hoc, ai soggetti sopra indicati: a) una descrizione della natura delle strategie di negoziazione algoritmica; b) i dettagli sui parametri o sui limiti di negoziazione a cui il sistema è soggetto; c) i controlli di conformità e di rischio attuati per assicurare che le condizioni stabilite al comma 1 siano soddisfatte; d) i dettagli sulla verifica dei sistemi; e) ulteriori informazioni sulla negoziazione algoritmica effettuata e sui sistemi utilizzati*".

[88] Il Rapporto Finale è disponibile all'indirizzo https://www.esma.europa.eu/sites/default/files/library/esma70-156-4572_mifid_ii_final_report_on_algorithmic_trading.pdf.

(comprese le società HFT) che applicano le loro strategie nelle sedi di negoziazione dell'UE; (*iii*) i requisiti organizzativi per le imprese di investimento, compresi i requisiti di notifica e verifica degli operatori algoritmici alle autorità competenti; e, gli esercizi di autovalutazione che devono essere eseguiti dalle imprese di investimento; (*iv*) i requisiti organizzativi per le sedi di negoziazione, compresi gli esercizi di autovalutazione che devono essere eseguiti dalle sedi di negoziazione, gli interruttori di circuito, le strutture tariffarie, i rapporti order to trade e interruzioni del mercato; e (*v*) una revisione delle disposizioni della MiFID II che sono indirettamente correlate alle attività di negoziazione algoritmica (ad es. *tick size e market making*).

6. La prospettiva dei penalisti.

La ricerca dei penalisti in Italia si è posta, almeno in questa fase, entro una prospettiva puramente teorica. Occorre chiarire anzitutto come il ventaglio di studi si proietti verso molteplici prospettive, sia processuali che sostanziali.

Sul primo versante vengono in rilievo questioni legate all'utilizzo della intelligenza artificiale nelle indagini preliminari, in particolare rispetto ai mezzi di ricerca della prova, e nella fase del giudizio finanche rispetto alla assunzione della decisione.

Sul versante sostanziale le questioni sono legate alla posizione dei sistemi di intelligenza artificiale, come autori (o coautori) del reato, vittime di esso, nonché al meccanismo di imputazione della responsabilità.

In questa sede è il versante sostanziale che interessa. Nell'ambito degli illeciti di manipolazione del mercato il tema è quello di verificare il livello di utilizzo o di interferenza rispetto all'azione umana. Appare pacifico che un sistema di intelligenza artificiale non possa divenire in quanto tale (certamente non lo possa oggi) centro di imputazione di responsabilità. Ipotesi di assimilazione alla responsabilità amministrativa degli enti appaiono del tutto improprie. Possono configurarsi profili di responsabilità penale (e, ove ne ricorrano i presupposti, profili di responsabilità dell'ente), quando il sistema di intelligenza artificiale venga programmato o utilizzato per la realizzazione di reati. I casi enucleati nel par. 4, descrittivi di una interazione di uomini e macchine, ne costituiscono esempi paradigmatici.

L'area problematica si pone rispetto agli strumenti muniti di un elevato grado di automazione (intelligenze di quarto livello, *machine learning*) nei quali la capacità di determinazione della macchina prescinde da impulsi diretti dell'uomo. In tali casi i profili di responsabilità possono porsi a posteriori, in relazione alla mancata attivazione dell'uomo per la prevenzione dell'illecito: in ipotesi, dovrebbe configurarsi una posizione di garanzia in capo al soggetto – produttore / titolare / utilizzatore – dello strumento di intelligenza artificiale, in funzione di controllo, per evitare o rimuovere gli effetti lesivi dell'azione dell'intelligenza artificiale. Riemerge, dai meandri del passato, la categoria dell'*actio libera in causa*.

È prevedibile, tuttavia, che i problemi di accertamento della responsabilità siano di estrema complessità, soprattutto sul piano soggettivo: anche quando l'illecito sia

provato nella sua componente oggettiva, possono restare incerti i confini della attribuzione soggettiva del fatto, soprattutto nella sua variante psicologica di volontà e rappresentazione. È stata evocata, a questo fine, la possibilità di procedere nei confronti dell'ente, facendo leva sull'art. 8 d.lgs. 231/2001 (autonomia della responsabilità dell'ente).

Nella grande ampiezza di prospettive appare significativo sottolineare come la riflessione nel diritto penale sia fortemente influenzata da istanze eticizzanti. La macchina non può sostituirsi (completamente) all'uomo, questo il motivo che accomuna i diversi percorsi argomentativi. E ciò sembra valere sempre, nel processo – ove il procedimento di assunzione della prova come quello decisionale non può fare astrazione dalla partecipazione e controllo del giudice – come anche nel diritto penale sostanziale, ove i principi sull'accertamento della responsabilità devono restare saldi. L'intelligenza artificiale pone nuovi problemi, applicativi ed interpretativi, ma la soluzione di essi deve trovare risposta nei confini del diritto penale nel nostro ordinamento democratico[89].

[89] Alcuni riferimenti bibliografici: I. SALVADORI, *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale*, in *Rivista italiana di diritto e procedura penale*, 1/2021; C. BARBARO, *Lo studio di fattibilità di un nuovo quadro normativo sulla concezione, lo sviluppo e l'applicazione dei sistemi di Intelligenza Artificiale sulla base delle norme del Consiglio d'Europa – Il lavoro del Comitato Ad hoc sull'intelligenza artificiale del Consiglio d'Europa (CAHA.I.)*, in *Questione Giustizia online*; M. PALMISANO, *L'abuso di mercato nell'era delle nuove tecnologie. Trading algoritmico e principio di personalità dell'illecito penale*, in *Diritto penale contemporaneo*, 2/2019; F. CONSULICH, *Il nastro di MÖBIUS. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato*, in *Banca Borsa e Titoli di Credito*, 2/2018.

Criptovalute, aspetti investigativi e processuali

di Fabio Di Vizio
Sostituto Procuratore presso il Tribunale di Firenze

SOMMARIO: Premessa. – 1. Attuale inquadramento normativo a livello nazionale delle valute virtuali e dei servizi relativi al loro utilizzo. – 1.1. Definizioni. – 1.2. Normativa antiriciclaggio nazionale. – 1.3. I limiti della riserva di attività. – 1.4. Il monitoraggio fiscale. – 2. Aree esposte a rischio di utilizzi criminali e di impieghi riciclatori: dagli ATM alla clientela dei prestatori di servizi relativi all'utilizzo di valuta virtuale e di portafogli digitali. – 3. Qualificazioni penali, tra reati presupposto, antiriciclaggio e riciclaggio: cenni. – 4. L'identificazione dei titolari effettivi e le indagini sulla *blockchain*: cenni sulla c.d. "*bitcoin forensics*". – 4.1. (*segue*) Evidenza investigativa della difficoltà di tracciare i dati qualificanti delle transazioni in valute virtuali con gli strumenti dell'analisi forense in caso di coinvolgimento di *exchange* centralizzati. – 5. Sequestri di criptovalute. – 5.1. Panoramica delle questioni sul sequestro di *bitcoin*. – 5.2. L'esperienza fiorentina. – 6. La giurisdizione, con particolare riferimento al riciclaggio mediante criptovalute.

Premessa.

Le note che seguono non hanno pretesa alcuna di completezza. Mirano esclusivamente a porre in evidenza le principali criticità cui si espone l'efficacia delle indagini e la praticabilità della celebrazione dei processi rispetto a reati coinvolgenti l'impiego di criptovalute, intendendo per questi ultimi quelli che ne sfruttano le caratteristiche di pseudo-anonimato e di a-territorialità e l'attitudine a realizzare rapidissimi, disintermediati, fiduciari e occulti trasferimenti tra diversi soggetti e differenti giurisdizioni territoriali.

Si muove dalla disciplina normativa apprestata per la materia, per censirne il carattere "difensivo" – si evoca in tal senso la figura delle cinte murarie da rinforzare e presidiare – rispetto a una nuova "realtà" economica deliberatamente sorta al di fuori degli assetti regolamentari e, allo stato, intercettata dai regolatori più che per i bisogni di tutela – il cui riconoscimento è sinora affidato quasi esclusivamente alla responsabilità del "diritto giudiziale"[90] – per i rischi di impiego e di propagazione rispetto ad operatività illecite. Con definizione di intese "diplomatiche" assai prudenti. Ne costituisce segno la circostanza per cui è stata la normativa antiriciclaggio la prima a considerare le valute virtuali, al pari del fatto che la stessa riserva di attività è concepita

[90] Per una panoramica dei principali approdi giurisprudenziali si rinvia a DI VIZIO F., *Lo statuto penale delle valute virtuali: le discipline e i controlli*, 19 giugno 2019, consultabile su https://discrimen.it/lo-statuto-penale-delle-valute-virtuali-le-discipline-e-i-controlli/. Si precisa che, coerentemente con la funzione di documento di lavoro, non destinato alla pubblicazione, il presente elaborato non contiene immancabili riferimenti a tutte le fonti della letteratura in materia delle quali pure è debitore.

in prospettiva di censimento degli intermediari e non di verifica della loro credibilità patrimoniale.

Resta il dato che questa cautela dei regolatori nel disciplinare il fenomeno e nell'acquisire la responsabilità del controllo, peraltro obiettivamente complicato, mantenendo letture tradizionali non adattabili ad un fenomeno tecnologico originale ne favorisce possibili interferenze con aree criminali, capaci di strumentalizzarne le caratteristiche, sfruttando le vaste opacità che il medesimo favorisce: le indagini e la stessa condizione di celebrazione devono calibrarsi su una realtà "virtuale" nuova, senza figurarsene una tradizionale immaginaria.

1. Attuale inquadramento normativo a livello nazionale delle valute virtuali e dei servizi relativi al loro utilizzo.

1.1. Definizioni.

Il d.lgs. 4 ottobre 2019, n. 125 ha specificato alcune definizioni contenute nel d.lgs. n. 231/2007. Anzitutto, ha aggiornato la definizione di valuta virtuale (art. 1, comma 2, lett qq, d.lgs. n. 231/2007) chiarendo che essa identifica la rappresentazione digitale di valore, non emessa né garantita (primo elemento innovativo) da una banca centrale o da un'autorità pubblica e che può essere utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalità d'investimento (secondo elemento innovativo).

Per la definizione di prestatore di servizi relativi all'utilizzo di valuta virtuale viene recepito quanto richiesto dagli standard GAFI. È tale ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale anche *online*, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale o in rappresentazioni digitali di valore, ivi comprese quelle convertibili in altre valute virtuali nonché i servizi di emissione, offerta, trasferimento e compensazione e ogni altro servizio funzionale all'acquisizione, alla negoziazione o all'intermediazione nello scambio delle medesime valute (cfr. la rivisitata lettera ff dell'art. 1, comma 2, d.lgs. n. 231/2007).

Attraverso l'innesto di una nuova lettera ff-bis) nell'art. 1, comma 2, d.lgs. n. 231/2007, viene introdotta la definizione di prestatore di servizi di portafoglio digitali: «*ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, anche online, servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali*». Si includono in tal modo anche tali soggetti tra i destinatari di obblighi di collaborazione attiva (abrogando la specificazione limitativa prevista in seno all'art. 3, comma 5, d.lgs. n. 231/2007 che riservava tale sottoposizione ai prestatori che svolgevano l'attività di conversione di valute virtuali da ovvero in valute aventi corso forzoso).

1.2. Normativa antiriciclaggio nazionale.

Il d.lgs. n. 90/2017 ha innestato nella categoria degli operatori non finanziari soggetti alle disposizioni del decreto antiriciclaggio (art. 3, comma 5, lett. i, d.lgs. n. 231/2007) i prestatori di servizi relativi all'utilizzo di valuta virtuale. Tale attrazione, però, inizialmente non è stata generalizzata, ma è avvenuta «limitatamente allo svolgimento dell'attività di conversione di valute virtuali da ovvero in valute aventi corso forzoso». Il riferimento, dunque, è stato riservato solo agli *exchange* che operano conversioni rispetto a valute aventi corso forzoso; tipica area di interferenza con la c.d. economia "reale".

Tale previsione ha aperto la strada alla possibilità di applicare le sanzioni amministrative e penali previste dal d.lgs. n. 231/2007 agli *exchange* tra valute virtuali e aventi corso forzoso ed ai loro clienti. Fuori però dell'ipotesi esaminata e di quelle in cui il servizio comporti la conversione di valute virtuali da ovvero in valute aventi corso forzoso non potevano ipotizzarsi violazioni antiriciclaggio, neppure collegate alle limitazioni in relazione all'uso del denaro contante (art. 49 d.lgs. n. 231/2007); comune è l'opinione che a tale ultima fattispecie non siano assimilabili le valute virtuali.

Lo pseudo-anonimato delle valute virtuali non agevola l'assolvimento degli obblighi di adeguata verifica (ai sensi dell'art. 18 d.lgs. n. 231/2007), specie con riferimento all'identificazione del titolare effettivo. Inoltre, alla diversa natura degli *exchange* corrispondevano anche diverse problematiche: gli *exchange* che imponevano il contatto fisico con il cliente potevano seguire le normali procedure di adempimento, mentre quelli virtuali restavano «nel limbo» dato che la previsione di identificazione a distanza necessitava di idonee forme e modalità (art. 19, comma 1, n. 5, d.lgs. n. 231/2007) che le autorità di settore dovevano ancora definire. In data 30 luglio 2019 è stato poi pubblicato il provvedimento della Banca d'Italia avente ad oggetto «disposizioni in materia di adeguata verifica della clientela per il contrasto del riciclaggio e del finanziamento del terrorismo». Il testo prevede nella Parte II Sezione VIII disposizioni specifiche in materia di operatività a distanza ed all'allegato n. 3 in tema di procedura di video-identificazione.

La lettera i) dell'art. 3, c.5, d.lgs. n. 231/2007 è stata modificata dall'art. 1, comma 1, lett. n), n. 4), d.lgs. 4 ottobre 2019, n. 125, eliminando l'inciso «limitatamente allo svolgimento dell'attività di conversione di valute virtuali da ovvero in valute aventi corso forzoso». Inoltre, L'*art. 1, comma 1, lett. n), n. 5), D.Lgs. 4 ottobre 2019, n. 125* ha aggiunto la lettera i-bis) ricomprendo tra i soggetti non finanziari soggetti alle disposizioni del decreto antiriciclaggio "i prestatori di servizi di portafoglio digitale".

Nel sistema preventivo dell'antiriciclaggio, all'estensione ai prestatori di servizi relativi all'utilizzo di valuta virtuale e ai prestatori ti servizi di portafoglio digitale dei doveri di collaborazione passiva ed attiva consegue l'introduzione degli obblighi, presidiati da sanzioni amministrative: i) di astensione dall'instaurazione, dall'esecuzione ovvero dalla prosecuzione del rapporto, della prestazione professionale e delle operazioni ex art. 43 d.lgs. n. 231/2007 allorché si trovino nell'impossibilità oggettiva di effettuare l'adeguata verifica della clientela (artt. 42, 19, comma 1, lettere a), b) e c), 56, comma 3, d d.lgs. n. 231/2007); ii) di conservazione dei dati, dei documenti e

delle informazioni previste per l'adeguata verifica (cfr. artt. 31, 32, 57 d.lgs. n. 231/2007); iii) di segnalazione delle operazioni sospette (cfr. artt. 35 e 58 d.lgs. n. 231/2007).

1.3. I limiti della riserva di attività.

Il d.lgs. n. 90/2017 ha stabilito l'obbligo dei *prestatori di servizi relativi all'utilizzo di valuta virtuale* (art. 1, comma 2, lettera ff), d.lgs. n. 231/2007) di iscriversi presso il registro degli agenti in attività finanziaria e dei mediatori creditizi, gestito dall'Organismo di vigilanza previsto dall'art. 128-undecies, d.lgs. n. 385/1993. Ai sensi dell'art. 8, comma 1, d.lgs. n. 90/2017 al decreto legislativo 13 agosto 2010, n. 141, all'art. 17-bis, dopo il comma 8, sono aggiunti i seguenti: «*8-bis. Le previsioni di cui al presente articolo si applicano, altresì, ai prestatori di servizi relativi all'utilizzo di valuta virtuale, come definiti nell'art. 1, comma 2, lettera ff), del decreto legislativo 21 novembre 2007, n. 231, e successive modificazioni tenuti, in forza della presente disposizione, all'iscrizione in una sezione speciale del registro di cui al comma 1. 8-ter. Ai fini dell'efficiente popolamento della sezione speciale di cui al comma 8-bis, con decreto del Ministro dell'economia e delle finanze sono stabilite le modalità e la tempistica con cui i prestatori di servizi relativi all'utilizzo di valuta virtuale sono tenuti a comunicare al Ministero dell'economia e delle finanze la propria operatività sul territorio nazionale. La comunicazione costituisce condizione essenziale per l'esercizio legale dell'attività da parte dei suddetti prestatori. Con il decreto di cui al presente comma sono stabilite forme di cooperazione tra il Ministero dell'economia e delle finanze e le forze di polizia, idonee ad interdire l'erogazione dei servizi relativi all'utilizzo di valuta virtuale da parte dei prestatori che non ottemperino all'obbligo di comunicazione*». Ai sensi dell'art. 17-bis, comma 1, d.lgs. n. 141/2010 «*l'esercizio professionale nei confronti del pubblico dell'attività di cambiavalute, anche su base stagionale, consistente nella negoziazione a pronti di mezzi di pagamento in valuta, è riservato ai soggetti iscritti in un apposito registro tenuto dall'Organismo previsto dall'art. 128-undecies del decreto legislativo 1° settembre 1993, n. 385*». L'esercizio abusivo dell'attività di cui al comma 1 è punita con una sanzione amministrativa da 2.065 euro a 10.329 euro emanata dal Ministero dell'economia e delle finanze (art. 17-bis, comma 5, cit.). In tal modo vengono create le premesse di un censimento delle piattaforme di scambio e dei gestori di portafogli elettronici oltre che di una riserva di attività sulla quale edificare doveri di collaborazione passiva ed attiva dell'antiriciclaggio. Ciò in funzione dell'istituzione di una banca dati centrale affidata al monitoraggio dell'UIF nella quale registrare l'identità degli utenti e gli indirizzi dei portafogli.

L'obbligo di iscriversi presso il registro degli agenti in attività finanziaria e dei mediatori creditizi, gestito dall'Organismo previsto dall'art. 128-undecies, d.lgs. n. 385/1993 viene espressamente riferito ai *prestatori di servizi di portafoglio digitali*, ritenendo, evidentemente, non del tutto perspicuo il precedente riferimento ai prestatori di servizi relativi all'utilizzo di valuta virtuale. Il decreto del Ministero dell'economia e delle finanze dovrà disciplinare le modalità e la tempistica dell'efficiente popolamento della sezione speciale dell'OAM, oltre che per i prestatori di servizi relativi all'utilizzo di valuta virtuale, anche per tale tipologia di prestatori di servizi, parimenti tenuti a comunicare al ricordato Ministero dell'economia e delle finanze la propria operatività

sul territorio nazionale, condizione essenziale per l'esercizio legale dell'attività da parte dei suddetti prestatori

1.4. Il monitoraggio fiscale.

In materia di monitoraggio fiscale, l'art. 1, comma 1, del d.l. n. 167/ 1990 (come sostituito dall'art. 8, comma 7, lett. a), d.lgs. 25 maggio 2017, n. 90) ha onerato proprio gli *exchange*, quali operatori non finanziari di cui all'art. 3, comma 5, lettera i), del decreto legislativo 21 novembre 2007, n. 231 (al pari degli intermediari bancari e finanziari di cui all'art. 3, comma 2, gli altri operatori finanziari di cui all'art. 3, comma 3, lettere a) e d)) «che intervengono, anche attraverso movimentazione di conti, nei trasferimenti da o verso l'estero di mezzi di pagamento di cui all'art. 1, comma 2, lettera s), del medesimo decreto a trasmettere all'Agenzia delle entrate i dati di cui all'art. 31, comma 2, del menzionato decreto, relativi alle predette operazioni, effettuate anche in valuta virtuale, di importo pari o superiore a 15.000 euro, indipendentemente dal fatto che si tratti di un'operazione unica o di più operazioni che appaiano collegate per realizzare un'operazione frazionata e limitatamente alle operazioni eseguite per conto o a favore di persone fisiche, enti non commerciali e di società semplici e associazioni equiparate ai sensi dell'art. 5 del testo unico delle imposte sui redditi, di cui al decreto del Presidente della Repubblica 22 dicembre 1986, n. 917».

Per la violazione degli obblighi di trasmissione all'Agenzia delle entrate previsti dall'art. 1, posti a carico degli intermediari, si applica la sanzione amministrativa pecuniaria dal 10 al 25% dell'importo dell'operazione non segnalata (art. 5, comma 1, d.l. n. 167/1990, convertito con modificazione dalla l. 227/1990). In base all'art. 2, comma 1, del d.l. n. 167/1990 (in vigore dal 4 luglio 2017) al fine di garantire la massima efficacia all'azione di controllo ai fini fiscali per la prevenzione e la repressione dei fenomeni di illecito trasferimento e detenzione di attività economiche e finanziarie all'estero, l'Unità centrale per il contrasto all'evasione fiscale (UCIFI) ed i reparti speciali della Guardia di Finanza possono richiedere — in deroga ad ogni vigente disposizione di legge, previa autorizzazione, rispettivamente, del direttore centrale accertamento dell'Agenzia delle entrate ovvero del Comandante generale della Guardia di finanza o autorità dallo stesso delegata — tra gli altri, agli *exchange* (operatori non finanziari di cui all'art. 3, comma 5, lettera i), del decreto legislativo 21 novembre 2007, n. 231, e successive modificazioni), di fornire evidenza, entro i limiti di carattere oggettivo stabiliti dall'art. 1, comma 1, del decreto, delle operazioni intercorse con l'estero anche per masse di contribuenti e con riferimento ad uno specifico periodo temporale nonché, con riferimento a specifiche operazioni con l'estero o rapporti ad esse collegate, l'identità dei titolari effettivi rilevata in applicazione dei criteri di cui all'art. 1, comma 2, lettera pp), e all'art. 20 del medesimo d.lgs. n. 231/2007. Almeno ai fini della disciplina del monitoraggio fiscale e della normativa antiriciclaggio, la valuta virtuale viene in rilievo quale mezzo di pagamento (art. 1, comma 1, d.l. n. 167/1990) e segnatamente quale strumento che permette di trasferire, movimentare o acquisire, anche per via telematica, fondi, valori o disponibilità finanziarie (art. 1, comma 2, lett. s, d.lgs. n. 231/2007). Quanto alle normative sul

monitoraggio fiscale (d.l. 28 giugno 1990, n. 167 in tema di rilevazione a fini fiscali di taluni trasferimenti da e per l'estero di denaro, titoli e valori), in materia valutaria (d.lgs. 19 novembre 2008, n. 195, contenente modifiche ed integrazioni alla normativa in materia valutaria in attuazione del regolamento CE n. 1889/2005) e sul monitoraggio antiriciclaggio (art. 49 d.lgs. n. 231/2007), la loro applicabilità è incisa dalle premesse qualificatorie sulla natura giuridica della valuta virtuale. Parificare la valuta virtuale al denaro contante importerebbe limiti al suo utilizzo e al suo trasferimento (cfr. art. 49 d.lgs. n. 231/2007) e obblighi di dichiarazione all'Agenzia delle Dogane dei movimenti transfrontalieri nella Comunità europea o in uscita da essa in caso di trasferimenti transfrontaliero di controvalore superiore a 10.000 euro (cfr. art. 3 d.lgs. n. 195/2008), ma non la sottoposizione al monitoraggio fiscale previsto dal d.l. n. 167/1990 per gli investimenti e le attività all'estero. Si è ritenuto che fossero equiparazioni sfornite di base legale, posto il carattere non solutorio (almeno non forzoso) della prima. La norma assume ad esclusivo riferimento gli *exchange* che si iscriveranno nell'apposita sezione dell'albo dei cambiavalute. Situazione che renderà ancor più irrazionale la previsione che ricollega una sanzione amministrativa mite alle attività degli *exchange* abusivi (da 2.065 euro a 10.329 euro) ed una potenzialmente molto alta (fino al 25% dell'importo dell'operazione non segnalata) per le omissioni nella trasmissione all'Agenzia delle Entrate dei dati di interesse per il monitoraggio fiscale da parte degli *exchange* iscritti. Irrazionalità che si manifesterà nel momento in cui il sistema previsto con la novella del 2017 entrerà a regime, con la pubblicazione del decreto ministeriale ex art. 17-bis d.l. n. 141/2010.

2. Aree esposte a rischio di utilizzi criminali e di impieghi riciclatori: dagli ATM alla clientela dei prestatori di servizi relativi all'utilizzo di valuta virtuale e di portafogli digitali.

L'analisi nazionale dei rischi di riciclaggio di denaro e di finanziamento del terrorismo elaborata dal Comitato di sicurezza finanziaria già nel 2018 testimoniava il grado di preoccupazioni delle Autorità in merito al pericolo di riciclaggio associato all'uso delle criptovalute. L'analisi dedicava un *focus* alle valute virtuali, rilevando come dalle evidenze investigative emerga un loro limitato utilizzo per acquisti di droga e di armi, per estorsioni e frodi informatiche nonché per operazioni di riciclaggio. Più che una realtà attuale, emergeva la percezione di un elevato grado potenziale di rischio e si richiamava la necessità di maggiore attenzione all'uso di asset virtuali supportato dalla tecnologia in continua evoluzione.

La relazione annuale per il 2018 della DNAA segnalava come ulteriori dati d'interesse le modalità di compravendita dei *bitcoin*, la quale può essere effettuata attraverso macchine collegate a internet, denominate *bitcoinATM*, che offrono la possibilità, mediante l'installazione di un'applicazione su apparati informatici (computer/tablet o smartphone), di procedere sia all'acquisto che alla vendita della cripto-valuta. Vengono poi in rilievo le procedure di scambio dirette tra utenti, mediante: — le più comuni piattaforme di commercio online tra privati (es. Ebay); —

transazioni "nascoste", effettuate nel deep web; — transazioni eseguite con l'ausilio di piattaforme web gestite da soggetti terzi che operano come intermediari "di fatto". Anche la nuova disciplina antiriciclaggio nulla dispone sullo scambio di valute virtuali tra pari utenti del circuito di pagamento elettronico (peer to peer) e sull'intermediazione operata dai *miners*, ossia coloro che validano le transazioni del sistema.

Devono essere considerate, inoltre, alcune conseguenze dell'impostazione originaria della disciplina antiriciclaggio nazionale, che, come visto, ha inteso organizzarsi anzitutto sulla responsabilizzazione dei cambiavalute virtuali. In primo luogo, infatti, l'identificazione dell'utenza era ritenuta essenziale rispetto al cambio della moneta legale in valuta virtuale e viceversa, non in relazione al pagamento con valute virtuali. Così solo le piattaforme di cambio erano tenute a comunicare all'autorità pubblica le operazioni "sospette". Rispetto alle operazioni di pagamento la pseudonimia degli utenti sembrava compensata dalla tracciabilità delle transazioni e dei codici identificativi degli utenti, garantita dalla tecnologia *blockchain*. L'incremento della diffusione del pagamento con valute virtuali — quali sistemi istantanei nei quali le transazioni non sono gestite da banche o altri intermediari qualificati ma da un registro delle transazioni (*blockchain*) decentrato e paritetico (*peer to peer*) — ha indotto a riconsiderare l'impostazione; in particolare *bitcoin* si è attestato tra i primi dieci sistemi di pagamento al mondo dopo Visa, MasterCard e PayPal. La circolazione monetaria, pur tracciabile attraverso la *blockchain*, non rende immediata l'identificazione dell'utenza. In ogni caso, numerose e vaste sono le aree in cui l'operatività in valute virtuali, anche ove siano coinvolti servizi dei cambiavalute, ha palesato il pericolo di impieghi riciclatori, in relazione a capitali opachi, utilizzo di schemi fiduciari dissimulati e di meccanismi collaterali.

Una di queste aree è rappresentata dal finanziamento alle imprese attraverso offerte iniziali di moneta *(initial coin offerings*). Sovente, infatti, *start up* innovative nel settore fintech sovvenzionano la propria attività emettendo gettoni (*token*) in cambio di moneta legale o valuta virtuale. Di frequente l'attività di impresa dell'emittente è in fase di mera progettualità e l'inizio della produzione di beni/prestazione di servizi è programmato dopo la conclusione della raccolta di fondi. Per sostenere un progetto — la creazione di un circuito monetario virtuale alternativo o un'iniziativa economica basata sulla tecnologia *blockchain* — alla pubblicazione on line di un prospetto informativo (*white paper*) segue la raccolta fondi (a termine, in moneta legale o in valuta virtuale) con susseguente rilascio di un *token* in favore del "pagatore", in misura proporzionale alla partecipazione al capitale di rischio richiesto per l'esecuzione del programma. I veicoli che emettono i *token* possono essere società, persone fisiche o *network* di sviluppatori di prodotti. I *token*, quale valuta virtuale di nuova emissione, saranno spendibili nel futuro sistema monetario virtuale, senza attribuire diritti sociali partecipativi, anche se l'emittente talvolta promette ai finanziatori forme diverse di condivisione dell'attività d'impresa, prospettandone i profitti. La raccolta dei fondi nell'ambito delle ICO di solito avviene in valuta virtuale e comporta di conseguenza l'esigenza, da parte del soggetto che ha lanciato la ICO, di cambiare la valuta virtuale in valuta fiat (che dovrebbe essere utilizzata per la realizzazione del progetto imprenditoriale). Spesso, inoltre, i *token* emessi in sede di ICO costituiscono a loro volta

asset virtuali che è possibile scambiare presso taluni *exchange*. Si tratta di un fenomeno economico che nel periodo di massimo valore delle valute virtuali ha consentito di raccogliere ingenti quantità di capitali (nel solo biennio 2017-2018 la raccolta a livello mondiale ha raggiunto quasi USD 30 mld). La collocazione tra il pubblico di nuove valute virtuali con tale schema di offerta richiede una scrupolosa adeguata verifica "in entrata", secondo la vigente disciplina antiriciclaggio (art. 17 d.lgs. n. 231/2007). È possibile che vengano destinati ad una ICO flussi finanziari di provenienza illecita; in altre parole, la ICO può essere sottoscritta mediante utilizzo di capitali di provenienza illecita, in assenza, allo stato, di una normativa uniforme in materia di obblighi di adeguata verifica sui sottoscrittori. È possibile, poi, che un soggetto giustifichi le proprie ingenti disponibilità in valuta virtuale sostenendo, in maniera non veritiera, di averle raccolte mediante il lancio di una ICO. Al riguardo, infatti, è complicato quantificare l'effettivo ammontare raccolto mediante la ICO nonché tracciare la provenienza della valuta virtuale, in assenza di figure professionali ovvero di soggetti vigilati che possano effettuare verifiche ed emettere le relative certificazioni.

Altre figure di clientela di interesse è quella degli investitori per conto terzi: i c.d. collettori. La diffusione delle valute virtuali, di pari passo con l'aumento delle quotazioni, ne ha comportato il proliferare. I "collettori", sovente già in possesso di pregresse esperienze di investimento in valute virtuali a titolo personale, hanno messo le loro conoscenze a disposizione di una cerchia, più o meno ampia, di potenziali investitori fungendo da punti di raccolta di fondi in valuta fiat, per investirli in valuta virtuale. Spesso la promozione dei servizi offerti dai collettori avviene mediante internet (siti, blog a tema, ecc.) e la raccolta dei fondi viene effettuata con la ricarica di carte prepagate. Tale attività è assimilabile a quella di un *exchange* professionale ma non di rado è effettuata in assenza di una adeguata struttura organizzativa che assicuri la tutela della clientela e il rispetto delle disposizioni normative antiriciclaggio. L'operatività dei "collettori" e delle piattaforme presenta evidenti rischi di riciclaggio in quanto si tratta di soggetti che, mediante la loro interposizione, non rendono conoscibile all'*exchange* ufficiale l'effettivo titolare delle somme investite in valute virtuali.

Vi è poi la figura degli arbitraggisti. Le valute virtuali possono essere negoziate su molte piattaforme diverse tra loro, non sempre soggette a regolamentazione, spesso operative 24 ore al giorno 365 giorni all'anno. Gli arbitraggisti guadagnano sfruttando i disallineamenti delle quotazioni nel cambio valute virtuali/valuta fiat presenti tra le varie piattaforme. L'attività, nella sua forma più semplice, si svolge mediante l'esecuzione "sequenziale" di operazioni di trading disposte manualmente e il trasferimento delle disponibilità tra le piattaforme coinvolte. Tale modalità produce tuttavia inefficienze derivanti dal costo delle commissioni sui molteplici trasferimenti tra le piattaforme. Tenuto conto dell'esigenza di mantenere ingenti disponibilità di valute virtuali sui rapporti, inoltre, i profitti possono essere erosi dall'elevata volatilità delle quotazioni. Tecniche più avanzate di arbitraggio, di converso, prevedono l'esecuzione "contemporanea" di operazioni di trading "opposte" sulle diverse piattaforme in modo da minimizzare sia l'importo delle disponibilità da detenere sui conti sia i trasferimenti da una piattaforma all'altra (che comunque si rendono necessari per riequilibrare eventuali sbilanciamenti). Spesso gli arbitraggisti più esperti si

avvalgono di software appositamente configurati (c.d. bot) che, grazie al collegamento alle varie piattaforme, riescono in automatico a inviare gli ordini di acquisto/vendita. Gli importi di valuta virtuale/fiat complessivamente movimentati sono molto ingenti, con centinaia di operazioni di trading giornaliere di ammontare singolo non particolarmente rilevante. La valutazione a fini antiriciclaggio dell'operatività degli arbitraggisti comporta diverse difficoltà concernenti la complessità della movimentazione (numero e vorticosità delle transazioni, numerosità delle valute virtuali coinvolte). L'utilizzo di molteplici piattaforme, seppur fisiologico per questa attività, complica la possibilità di tracciare i flussi al fine di ricostruire la provenienza dei fondi. Nell'ambito della propria attività, gli arbitraggisti hanno l'esigenza di spostare velocemente la valuta virtuale/valuta fiat da una piattaforma all'altra. Al riguardo, i trasferimenti di valuta virtuale avvengono mediante *blockchain*, mentre le transazioni di valuta fiat comportano generalmente la necessità di avvalersi dei sistemi di pagamento tradizionali, ovvero di utilizzare metodi alternativi di trasferimento quali le *stablecoin* ancorate a valute aventi corso legale.

Da alcune evidenze è emersa la possibilità degli utenti di detenere disponibilità su rapporti accesi presso la piattaforma di un *exchange*, sia in valuta virtuale sia in valuta fiat, funzionali all'attività di trading. Sovente le monete tradizionali sono detenute mediante intermediari finanziari abilitati su conto intestato all'*exchange*, assimilabile a un conto *omnibus*. Ciò ostacola l'intermediario abilitato, all'oscuro delle disponibilità in valuta legale riconducibili ai singoli clienti dell'*exchange* ad una determinata data e affida solo alle eventuali procedure di monitoraggio di quest'ultimo la registrazione delle disponibilità presenti sui conti dei clienti. In tal modo, questi ultimi potrebbero detenere ingenti quantità di valute cripto e fiat, talvolta anche per lunghi periodi e senza utilizzarle per attività di trading. Tale circostanza determina, in ragione dell'assenza, tuttora attuale, in capo all'*exchange* degli obblighi di comunicazione previsti per l'archivio dei rapporti con operatori finanziari dell'Agenzia delle Entrate, la possibilità per i clienti della piattaforma di detenere disponibilità in euro su conti non censiti nel ricordato archivio.

Vi è ancora, l'evidenza problematica di trasferimenti "indiretti" di valuta fiat mediante rete *Ripple* e *stablecoin* (valute virtuali il cui valore è ancorato a valute legali). Talora i clienti dell'*exchange* possono trasferire valuta fiat mediante strumenti alternativi ai tradizionali servizi di pagamento, in particolare utilizzando *Ripple* ovvero *stablecoin*. Il prelievo di valuta fiat tramite *Ripple* avviene mediante l'emissione da parte dell'*exchange* di un *token* di pari valore. Tali *token*, possono essere scambiati all'interno della rete Ripple da chiunque ne sia in possesso e sono accettati dagli *exchange* che hanno riconosciuto come affidabile l'entità che li ha emessi, unico soggetto, tra l'altro, in grado di "riscattarli". A titolo esemplificativo, un utente dell'*exchange* che voglia trasferire euro dal proprio rapporto potrebbe richiedere allo stesso *exchange* l'emissione di un *token* di importo pari al valore che vuole trasferire. Questo *token*, poi, sarebbe trasferito informaticamente mediante la rete *Ripple* al beneficiario, il quale potrebbe in linea teorica

scambiarlo presso un altro *exchange* di valute virtuali[91] venendosi accreditate il corrispettivo in euro sul proprio rapporto (a condizione che accetti i *token* emessi dal primo *exchange*). Tale operatività può realizzarsi anche tra clienti diversi del medesimo *exchange*. Un'ulteriore opportunità per il trasferimento di valuta fiat deriva dall'utilizzo di asset virtuali (c.d *stablecoin*) il cui valore è ancorato a valute aventi corso legale, rappresentato da un *token* negoziabile anche presso alcuni scambiatori virtuali. A titolo esemplificativo il cliente che voglia trasferire dollari dal proprio rapporto in essere presso l'*exchange* potrebbe acquistare *stablecoin* utilizzando *bitcoin* o euro e poi trasferirli tramite *blockchain*. In questo caso, pur riguardando formalmente una valuta virtuale, il trasferimento nella sostanza è assimilabile a un'operazione in valuta fiat cui lo *stablecoin* ancorato. La possibilità di detenere e trasferire *stablecoin* ovvero la possibilità di trasferire valute fiat sfruttando i *Ripple* comporta rilevanti conseguenze sugli aspetti antiriciclaggio. Infatti, pur volendo limitare il monitoraggio delle transazioni a fini antiriciclaggio alle sole operazioni che interessano la valuta avente corso legale, andrebbero comunque quanto meno tenute in considerazione, oltre alle operazioni di cambio tra valuta fiat/valute virtuali, anche i trasferimenti e i cambi tra quelle valute virtuali che consentono di movimentare indirettamente valute fiat come gli IOU *Ripple* e le *stablecoin*.

Una criptovaluta che sembra prestarsi meglio dei *bitcoin* ad usi illeciti è Monero[92]. Creata nel 2014, essa viene pubblicizzata rimarcando l'attenzione per la privacy e la sicurezza. Infatti, è una criptovaluta non tracciabile e anonima, non potendo in alcun modo determinare se una transazione è stata realmente effettuata o tra chi è stata effettuata. Questo risultato viene ottenuto tramite adozioni tecnologiche differenti rispetto al *bitcoin*, dove le transazioni sono tracciabili ed è possibile almeno in linea teorica, risalire all'identità dei soggetti della transazione. Monero quindi è un esempio di come, a differenza di *Ripple*, sia stato sviluppato il funzionamento della *blockchain* per finalità comunque non trasparenti, seppure giustificate dall'esaltazione dei valori della privacy e della sicurezza delle transazioni. Anche *Zcash* è una criptovaluta strumentalizzabile a fini illeciti. Fondata da Zooko Wilcox-O'Hearn, offre *privacy* e trasparenza selettiva delle transazioni: i pagamenti Zcash sono pubblicati

[91] *Ripple* è un sistema di trasferimento fondi in tempo reale, basato su tecnologia *blockchain* sviluppata dall'omonima società statunitense. Tale sistema è stato disegnato per eseguire transazioni finanziarie internazionali e per tale motivo ha attirato l'interesse di diversi istituti bancari. Le transazioni *Ripple* possono essere eseguite attraverso gli XRP (la criptovaluta nativa di *Ripple*) o tramite il meccanismo degli IOU (I Owe yoU), *token* emessi e scambiati da specifici nodi della rete (i gateway), che consentono di veicolare qualunque tipo di valore (per esempio criptovalute o valute fiat).

[92] Oltre ai possibili utilizzi illeciti, Monero presenta delle caratteristiche addirittura vantaggiose per quanto riguarda la conformità delle disposizioni contenute nel GDPR (Regolamento UE 2016/679), infatti «Attualmente, le uniche criptomonete ad apparire potenzialmente conformi alle disposizioni del GDPR sono le c.d. privacy coin (come ad esempio Monero), che sembrano in grado di garantire un effettivo anonimato agli utilizzatori, in quanto non conservano all'interno della propria *blockchain* alcuna "personally identifiable information" (vale a dire informazioni che consentono di individuare l'utente all'interno del sistema)».

su una *blockchain* pubblica, ma il mittente, il ricevente e il valore della transazione possono rimanere privati.

3. Qualificazioni penali, tra reati presupposto, antiriciclaggio e riciclaggio: cenni.

Le valute virtuali si prestano ad essere utilizzate come "valuta" nella commissione dei *cybercrimes*, ossia quale forma di profitto al quale tendono i *cyber*-criminali; vengono utilizzate per il riciclaggio di denaro e richieste come "prezzo" da pagare nel caso delle estorsioni *on-line* (*phishing, sextortion, ransomware* etc.); la criptovaluta è anche la "moneta" utilizzata nel *dark web* per l'acquisito di beni la cui compravendita è proibita dalla legge.

L'anonimato delle transazioni regolate con valute virtuali, anche nella fase del trasferimento (non condizionato dall'identificazione delle controparti né da alcuna causale e realizzabile per importi assai elevati), la *natura ubiqua e l'estrema versatilità* delle criptovalute le rendono veicolo appetibile per fini illeciti. Numerose sono le aree in cui l'operatività in valute virtuali, pur laddove ove ad essere coinvolti siano i servizi dei cambiavalute e dei prestatori di portafogli digitali, ha già palesato il pericolo di impieghi riciclatori. Capitali opachi, schemi fiduciari dissimulati, meccanismi collaterali per il trasferimento nascosto delle risorse tradizionali sono realtà investigative allarmanti,

Contro tale possibile impiego, l'ordinamento reagisce con strumenti tipici del diritto penale senza vittima, a protezione di interessi diffusi e astratti presidiando anzitutto le condizioni di efficienza delle funzioni pubbliche di controllo. L'art. 55 d.lgs. n. 231/2007, ad esempio, accoglie le fattispecie penali incriminatrici delle violazioni più insidiose degli obblighi antiriciclaggio, rivisitate dalla novella del 2017 (v. infra). Non è un caso che la normativa (antiriciclaggio sia stata quella maggiormente pronta ad offrire considerazione delle valute virtuali. Accanto alla considerazione dei vantaggi per l'efficienza economica della nuova tecnologia informatica collegata alla *blockchain*, edificata sulla disintermediazione e predisponente a forme più diffuse di democrazia finanziaria, immediata è risultata la percezione della preoccupazione connessa al trasferimento, alla custodia ed agli impieghi illeciti delle risorse virtuali connotati da irreversibilità, anonimato (o pseudo-anonimato)) e infrastrutture complesse, tra diversi Stati e giurisdizioni con variegata sensibilità antiriciclaggio; condizioni che finiscono, obiettivamente, per favorire connessioni naturali tra le valute virtuali ed il mondo del crimine e del riciclaggio.

Nella relazione annuale per il 2018 della DNAA sono ben chiariti i termini del rischio sistemico collegato alla creazione nel web di un "paradiso finanziario virtuale". Questa prospettiva è agevolata dal fatto che: — il sistema delle cripto-valute ha natura decentralizzata, in cui ogni computer ha eguale accesso alle risorse comuni e ogni transazione risulta garantita e convalidata dagli stessi utenti; — le transazioni possono avvenire non soltanto tra soggetti residenti in Stati diversi, ma anche essere riconducibili a *più account* in realtà riferibili sempre alla medesima persona, potendo un unico utente risultare titolare di più account della medesima cripto-valuta contemporaneamente; — esistono sempre più espedienti capaci di assicurare un maggior grado di anonimato. Ad

esempio, è stato riscontrato l'utilizzo del meccanismo del c.d. *tumbler*, mediante il quale la transazione non è ricondotta all'account del soggetto agente, bensì a una molteplicità di account inesistenti». In questo contesto, il *bitcoin* risulta la prima moneta per i pagamenti realizzati sul *darknet* ovvero per il commercio illegale, le truffe, le varie *scams* nelle piattaforme di *mixing*, lo scambio di materiale pedopornografico, anche attraverso le richieste di crowdfunding per la copertura delle spese di viaggio o altro.

Come ricordato in dottrina «*nelle valute virtuali decentrate, la blockchain conserva la storia delle transazioni così da rendere possibile ricostruire tutte le operazioni eseguite, ma identifica gli utenti solo attraverso uno pseudonimo. Risalire da tale dato alla reale identità della controparte non è semplice e, considerato che la registrazione degli utenti al momento della generazione dell'indirizzo non è soggetta alle rigorose norme sull'adeguata verifica proprie della disciplina antiriciclaggio, non è affatto detto che il titolare possa mai essere identificato con certezza. Tale circostanza unita all'irrevocabilità delle transazioni eseguite con valuta virtuale potrebbe agevolare le frodi ai danni degli utenti*».

Sotto un profilo investigativo, la relazione riepiloga le difficoltà che incontrano le indagini aventi ad oggetto operatività in cripto-valuta: — la complicata identificabilità degli indagati; — la complessa acquisizione di prove circa le movimentazioni di valuta virtuale e la riconducibilità a soggetti specifici; — la concreta sequestrabilità delle *virtual currencies* e delle disponibilità presenti sui wallet».

Sino all'entrata in vigore della riforma del 2019 gli snodi nei quali si può intercettare l'identità relativa a chi si cela dietro una operazione in cripto-valuta sono i cc.dd. "punti di ingresso e di uscita dal circuito" (in particolare gli "*exchange*"), ossia nell'ambito del processo di conversione della cripto-valuta in valuta a corso legale e viceversa.

Tra le fattispecie antiriciclaggio merita ricordare il delitto previsto dall'art. 493-ter c.p. che offre occasione di tutela penale rispetto ad indebiti utilizzi delle chiavi crittografiche private utilizzate per trasferire valute virtuali dai portafogli digitali. Le chiavi in argomento possono porsi in connessione funzionale con l'acquisto di beni o servizi presso soggetti che accettino su base convenzionale tale modalità solutoria. In altre parole, possono integrare la figura di «*qualsiasi altro documento analogo che abiliti ... all'acquisto di beni o alla prestazione di servizi*». La migliore giurisprudenza qualifica nei termini di frode informatica ex art. 640-ter c.p. la condotta di colui che, servendosi di una carta di credito falsificata e di un codice di accesso fraudolentemente captato in precedenza, penetri abusivamente nel sistema informatico bancario ed effettui illecite operazioni di trasferimento fondi.

Le fattispecie previste dall'art. 55, comma 1 e 2, d.lgs. n. 231/2007, dopo la riforma del 2017, risultano incentrate attorno a condotte connotate da fraudolenza e decettività; condizioni che pongono problemi di delimitazione rispetto alle tradizionali fattispecie penali del riciclaggio. In tale contesto, «il crimine può avvalersi dei servizi di *mixing* (noti anche come *cryptocurrency tumbler*) e sfruttare complesse tecniche di trasferimento della valuta virtuale che, utilizzando conti di rimbalzo (conti *bounce*) o collettori (conti *pool* o pot) in combinazione con la tecnologia *blockchain* rendono quasi impossibile la ricostruzione dei passaggi intermedi [tra fase di ingresso (gateway) e uscita (withdrawing)], garantendone l'anonimato. La specificità di queste tecniche,

immediatamente riconducibile alla nota modale che contraddistingue la struttura penalistica del riciclaggio (art. 648-bis c.p.) consente sostituzioni o trasferimenti *"in modo da ostacolare la identificazione della provenienza" delle utilità eventualmente illecite, perché generate da un delitto non colposo*».

Il carattere pseudoanonimo (se non anonimo) dell'impiego della valuta virtuale (come nel caso dei *bitcoins*) in un'operazione di scambio, a basso costo e tra giurisdizioni diverse, ulteriormente aggravato da servizi di mixing, risultano condizioni obiettivamente predisponenti alle operazioni di riciclaggio. Non è un caso, del resto, che alcuni Paesi si siano attivati con normative che impongono l'identificazione dei soggetti cedenti o destinatari di valute virtuali[93] (198).

Il complicato inquadramento giuridico delle valute virtuali, con i riflessi sull'indecifrabilità delle correlative discipline di settore, appare meno significativo per i reati di riciclaggio, intendendo per essi quelli previsti dagli artt. 648-bis, 648-ter, 648-ter.1. c.p. Le condotte di tali fattispecie hanno quale elemento di origine (provento) o di trasformazione (prodotto) la componente delle utilità, con contenuto assai ampio. In particolare, secondo quanto anticipato, per la giurisprudenza di legittimità, con il progressivo ampliamento dei reati presupposto, della condotta incriminabile e dell'oggetto del reato, utilizzando la locuzione «altre utilità», il legislatore ha inteso colpire con il delitto di riciclaggio «ogni vantaggio derivante dal compimento del reato presupposto». Una clausola di chiusura rispetto al denaro ed ai beni impiegata proprio per evitare che sfuggano alla repressione penale utilità derivanti dal reato presupposto e delle quali l'agente, grazie all'attività di riciclaggio realizzata da un terzo, possa usufruire. Le utilità, dunque, quali valori economicamente apprezzabili, comprendono non solo gli elementi che incrementano il patrimonio dell'agente ma anche il frutto delle attività fraudolente a seguito delle quali si impedisce l'impoverimento del patrimonio. È utilità, ad esempio, anche il mancato decremento del patrimonio, ossia il risparmio di spesa realizzato evitando di pagare le imposte dovute attraverso la perpetrazione di un reato fiscale[94] .

---

[93] *Specifiche key disclosure laws* sono state approvate nel Regno Unito, in Australia ed in Sud Africa, arrivando a sanzionare con il carcere il rifiuto di rivelare alle autorità competenti le chiavi crittografiche alla base delle transazioni di interesse di queste ultime. In ragione del diffuso ricorso dello strumento di *bitcoin* per l'acquisto di beni illeciti o per il finanziamento di attività illecite alcuni paesi hanno vietato alle banche di accettare *bitcoins* (come la Russia o la Cina) nonché agli operatori del settore finanziario di realizzare attività ad essi collegati (Cina 2013), sino alla messa al bando dei *bitcoins* (decisa in Russia nel 2014).

[94] Recenti pronunce della Cassazione hanno avallato questa interpretazione, come nel caso della sentenza della II sezione penale n. 6061 del 17 gennaio 2012, dep. 15 febbraio 2012, Gallo, Rv 252701, che ha ammesso la configurabilità del delitto di frode fiscale quale reato presupposto del riciclaggio, in passato accennata in termini incidentali (Cass. pen. sez. VI, n. 45643 del 30 ottobre 2009, dep. 26 novembre 2009, Papale; Cass. pen., sez. II, n. 49427 del 17 novembre 2009, dep. 23 dicembre 2009, Iametti, Rv 246470; Id., n. 23396 del 11 maggio 2005, dep. 21 giugno 2005, Simonelli, Rv. 231884). La stessa ultima configurazione normativa del reato di riciclaggio, come visto, ha importato una significativa estensione della portata della fattispecie, ampliando i reati presupposti (delitti non colposi), la condotta, l'oggetto iniziale («altre operazioni» «in relazione» — e non su — a denari, beni ed utilità di provenienza delittuosa in modo da ostacolarne l'identificazione) e quello finale (potendo trattarsi, per tutte le condotte, di «denaro, beni, o altre utilità» ma anche di «cose» di diversa natura, pure sprovviste di valore economico, restando punibile anche la c.d.

Sembra chiaro, dunque, che anche la valuta virtuale, quale oggetto, strumento e prodotto del riciclaggio, sia un'utilità rilevante. Le condotte di riciclaggio devono essere connotate da attitudine decettiva. Si tratta dell'idoneità a complicare l'accertamento dell'identificazione della provenienza illecita del bene, senza necessariamente impedirlo definitivamente. Come visto, la giurisprudenza esclude che la ricostruibilità storica — a posteriori — delle transazioni e dei loro protagonisti digitali costituisca un impedimento assoluto all'integrazione del reato di riciclaggio; nel caso delle valute virtuali a non essere assicurato, infatti, è proprio il legame tra gli indirizzi delle transazioni e l'identità di chi realmente li controlla; onde assai sviluppata è la possibilità che il trasferimento e le sostituzioni valgano a complicare l'identificazione della provenienza delittuosa. In punto di configurabilità del reato di autoriciclaggio, di recente la Cassazione penale ha statuito che «nel concetto di "attività speculativa" di cui all'art. 648-ter.1 c.p. ben possano rientrare anche i giochi o le scommesse caratterizzati da azzardo (intendendosi per tali quelli praticati con fine di lucro e nei quali la vincita o la perdita sia in buona parte aleatoria» (Cass. pen., sez. II, n. 13795/2019; contra Cass. pen., sez. II, n. 9751/2019). Secondo il Collegio di legittimità (Cass. pen., sez. II, n. 30399/2018), tenuto conto della clausola di non punibilità prevista nel comma quarto dell'art. 648-ter.1 c.p. «l'agente può andare esente da responsabilità penale solo e soltanto se utilizzi o goda dei beni provento del delitto presupposto in modo diretto e senza che compia su di essi alcuna operazione atta ad ostacolare concretamente l'identificazione della loro provenienza delittuosa». La componente speculativa dell'investimento in valute virtuali può dunque integrare l'elemento oggettivo del reato in analisi.

4. L'identificazione dei titolari effettivi e le indagini sulla *blockchain*: cenni sulla c.d. "*bitcoin forensics*".

Il diffondersi dell'utilizzo delle criptovalute tra gli utenti e la loro crescente rilevanza nei *cybercrimes* accresce l'esigenza di condurre indagini efficienti, con tecniche investigative calibrate sulle loro caratteristiche strutturali e di funzionamento.

La *blockchain*, quale registro delle transazioni, è pubblica ed è detenuta da tutti i nodi della rete; ognuno può accedervi, consultare le transazioni iscritte ed estrarne una copia. Questa caratteristica è utile ai fini investigativi in quanto è possibile analizzare tutte le "movimentazioni" delle valute virtuali a ritroso fino alla prima mai avvenuta. Del resto, l'obiettivo della creazione del *bitcoin* non era il conseguimento della totale anonimità (con la finalità di occultare operazioni poco limpide), ma quello di raggiungere una sicura *privacy* nelle proprie movimentazioni di denaro (*privacy* intesa come diritto alla riservatezza con la possibilità, a discrezionalità del soggetto, di rivelare i propri dati), dando vita ad un sistema "*pseudo-anonimo*". Pertanto, la sostanziale "*ubiquità*" della *blockchain* è un elemento a favore degli investigatori in quanto non sarà

sostituzione "eterologa").

necessario, per accedere ai dati dei *server* locati in altre giurisdizioni, ricorrere a complesse operazioni coinvolgendo anche le autorità giudiziarie di altri paesi.

Alcune criptovalute (*Monero* e *ZCash*) per rafforzare la *privacy* degli utenti non prevedono una *blockchain* completamente trasparente, omettendo di indicare l'importo della transazione e/o gli indirizzi dei *wallet*. In particolare, *Zcash* permette di scegliere se rivelare per ogni transazione l'importo e gli indirizzi (come avviene con il protocollo *bitcoin*, *Ethereum* e le restanti criptovalute esistenti), oppure solo l'importo o uno dei due indirizzi; tutto ciò per facilitare gli utenti ad adempiere agli obblighi di *compliance* (in specie, gli obblighi antiriciclaggio) o di *audit*. L'utilizzo di tali criptovalute rende quasi impossibile qualsiasi operazione di indagine in quanto non consentono di disporrebbe, a fini investigativi, neanche degli estremi degli *address* e dell'importo trasferito.

Il protocollo *bitcoin*, invece, permette di analizzare lo storico delle transazioni, offrendo agli investigatori elementi per ricostruire la provenienza dei *bitcoin* o addirittura risalire ai titolati degli *address*.

La crittografia, utilizzata nelle *blockchain* per garantirne la sicurezza e la riservatezza, è strumentalizzata dai *cyber-criminali* al fine di impedire le attività delle autorità inquirenti o comunque frenarne notevolmente le indagini. I sistemi di crittografia avanzati non sono impossibili da decifrare, ma comportano l'impiego di ingenti risorse e di tempo, il che complica l'efficienza delle indagini e agevola i criminali nel far perdere le proprie tracce. È stato quindi sottolineato come una cooperazione dei produttori di beni e servizi[95] nell'ambito informatico o delle telecomunicazioni che utilizzano la crittografia sia estremamente necessaria per consentire alle unità investigative le dovute indagini essendo in possesso della chiave di decrittazione. Tuttavia, nel caso del protocollo *bitcoin* e delle altre criptovalute (ad eccezione di *Ripple*, la cui *governance* è centralizzata), non vi è un ente centrale con cui interfacciarsi o con cui confrontarsi nel caso in cui sia necessario condurre un'indagine che comporti la decrittazione di determinate informazioni. Si potrebbe pensare di instaurare rapporti con i *wallet providers* e gli *exchange* di criptovalute in modo tale da poter chiedere loro di fornire le informazioni – nel caso le abbiano – sui propri clienti. In effetti gli obblighi derivanti dalla V Direttiva antiriciclaggio di fatto impongono ai *wallet provider* di adottare misure di adeguata verifica e di segnalazione di operazioni sospette; pertanto, almeno nell'ambito dell'operatività delle norme dell'Unione europea la suddetta cooperazione tra privati e autorità investigative è stata adeguatamente regolata, anche se la collaborazione con le Autorità non è il criterio selettivo prioritario di tali operatori.

La c.d. *bitcoin forensics* – quale «*impiego di strumenti statistici per aggregare transazioni e identificare utenti*» – ha consentito di conseguire importanti risultati attraverso lo svolgimento di indagini sulla *blockchain*.

La letteratura in materia propone diverse metodologie di indagine, una delle quali consiste nella "*deanomization*" ("de-anonimizzazione"). Questa tecnica consiste nell'associare ad un *address* bitcoin l'identità di un soggetto, un indirizzo *e-mail*, un

[95] V. Il caso di *Blackberry*, che ha contrattato la cessione delle proprie chiavi di decrittazione in cambio dell'opportunità di operare nel territorio dei governi dei paesi contraenti.

numero di telefono o qualsiasi altra identità digitale (*username*, *account Google* ecc.). Possono essere distinte due categorie di metodi di *deanomization,* attivi e passivi. I *metodi attivi* consistono nell'utilizzo di tecniche di *social engineering* o nodi della rete *bitcoin* "malevoli". I metodi passivi invece, si limitano ad analizzare le transazioni pubbliche della *blockchain*. In particolare, i metodi di *social engineering* consistono nel cercare un diretto contatto con il soggetto in modo tale da scoprirne l'indirizzo *bitcoin* ad esso collegato. È attuabile, ad esempio, attraverso l'acquisto di un bene dal soggetto messo in vendita nei *dark markets*; è il metodo più efficace perché il venditore non fornirà informazioni false in quanto interessato a ricevere il pagamento ma può porre problemi di ammissibilità nei settori investigativi nei quali non sia disciplinata la facoltà di operare sotto-copertura o come agente provocatore. Un altro esempio, anch'esso squisitamente tecnico, è costituto dalla creazione di nodi della rete *bitcoin* con la finalità di intercettare le connessioni in entrata e quindi di rilevare l'indirizzo IP degli utenti che trasmettono le transazioni[96]. I *metodi passivi*, in particolare, sono costituiti da tecniche di analisi e indagine dello storico delle transazioni della *blockchain* che possono essere piuttosto sofisticate. Una delle tecniche consiste nell'accorpare (il c.d. "*clustering*"[97]) più indirizzi *bitcoin* appartenenti allo stesso soggetto analizzando l'*input* e l'*output* della transazione, notando che il primo comprende più *address*, ed il secondo è costituito da un solo indirizzo[98].

Le tecniche più complesse invece studiano le movimentazioni dei *bitcoin* cercando di individuare e di accorpare gli indirizzi che ricevono più "moneta" senza spenderla; in tal modo, si cerca di individuare gli *address* dei *dark markets* di siti di scommesse illegali. Oltre queste tecniche complesse, è discussa l'opportunità di ricorrere al c.d. *blacklisting*, ossia alla "marchiatura" dei *bitcoin* provenienti da soggetti noti per le loro attività illecite come ad esempio, tentativi di *phishing*, estorsioni *online* ecc. Addirittura, esistono piattaforme online (il più noto è "*bitcoinwhoswho*") finalizzati a raccogliere le segnalazioni di indirizzi *bitcoin* fraudolenti; così facendo, gli utenti possono verificare se un determinato indirizzo *bitcoin* è stato segnalato per aver commesso tentativi di frodi o *phishing*, contribuendo alla sicurezza della rete *bitcoin*. È possibile anche di propria iniziativa fornire i propri dati alla suddetta piattaforma in modo da poter garantire agli altri utenti di non essere implicati in operazioni illecite, e ciò può essere utile nel caso di venditori che accettino e utilizzino i *bitcoin* come corrispettivo.

L'utilizzo dei servizi di *mixing* rende estremamente più complesso, ma non impossibile, l'analisi delle transazioni della *blockchain*. Inoltre, utilizzo del *browser* TOR

---

96 Esistono, infatti, due tipologie di nodi nella infrastruttura della rete *peer to peer* del *bitcoin*: i *client* e i *server*. I *client* non accettano connessioni in entrata, mentre i *server* si. I nodi "malevoli", quindi, si andrebbero a configurare come nodi *server*, che quindi ricevono le connessioni in entrata costituite dalle transazioni.

97 *Online* è disponibile un sito web che permette di ricercare i *wallet* accorpati appartenenti allo stesso soggetto: v. *https://www.walletexplorer.com*

98 I portafogli *bitcoin* non cumulano su un unico conto la totalità dei *bitcoin*. Se si è in possesso di un portafoglio contenente 5 *bitcoin*, e si ricevono 4 *bitcoin*, si avrà un *wallet* costituito da due "sotto portafogli" rispettivamente di 5 e 4 *bitcoin*; non quindi un unico portafoglio contenente 9 *bitcoin*. La criptovaluta *Ethereum*, invece, accorpa tutti gli *ether* posseduti in un unico conto

e dei VPN può rendere vane le ricerche finalizzate all'individuazione dell'indirizzo IP che con i suddetti accorgimenti viene mascherato o sottoposto a stratificazione crittografica.

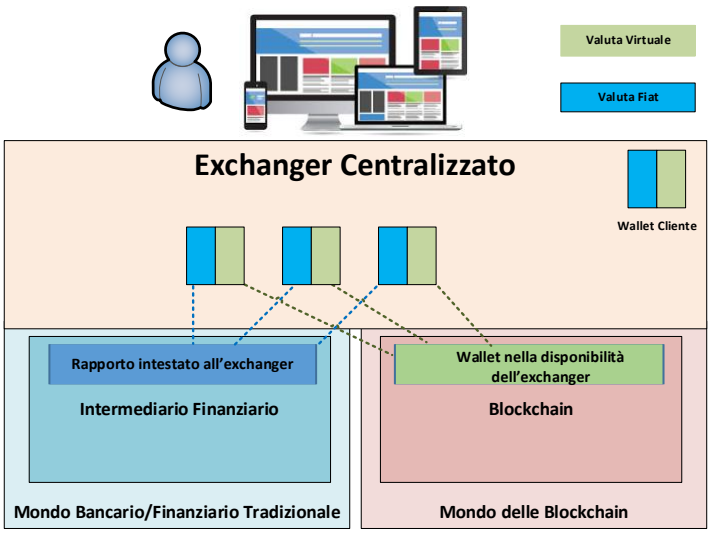
Quindi, se le indagini informatiche in generale presentano peculiarità in ordine all'oggetto delle indagini, le investigazioni relative alla criptovalute pongono nuove sfide agli inquirenti. L'utilizzo della crittografia, dei servizi di *mixing* e di *tumbling* rendono più complicato l'esperimento di indagini proficue, ma comunque sono in via di sviluppo tecniche di analisi che possano aggirare questi ostacoli.

4.1. (segue*) Evidenza investigativa della difficoltà di tracciare i dati qualificanti delle transazioni in valute virtuali con gli strumenti dell'analisi forense in caso di coinvolgimento di* exchange *centralizzati.*

La Procura di Firenze ha svolto approfondimenti in relazione ad una richiesta di rogatoria che si focalizzava, tra i vari elementi, su n. 3 indirizzi *bitcoin* sui quali sarebbero state trasferite disponibilità di origine illecita.

Tali indirizzi erano gestiti dagli *exchange* centralizzati, che di seguito di denomineranno H e O: al fine di meglio comprendere l'esito delle analisi condotte nonché gli eventuali ulteriori approfondimenti attivabili con particolare riguardo all'analisi delle transazioni in criptovaluta (c.d. *analisi forense delle transazioni*) è bene richiamare brevemente la logica di funzionamento di tale tipologia di operatori.

***Exchange* centralizzati**



Nel modello tecnologico-operativo degli *exchange* centralizzati il cliente della piattaforma non opera direttamente in *blockchain* e non controlla in autonomia le proprie disponibilità in valuta virtuale. In tale modello, infatti, il cliente accende presso un *exchange* un *wallet* (o *account*) e opera sulle proprie disponibilità esclusivamente

ricorrendo alle funzionalità offertegli, generalmente mediante siti Internet o App, dalla piattaforma che, contrariamente alla filosofia originaria delle valute virtuali, disintermedia completamente il cliente rispetto alla *blockchain* operando, in sostanza, alla stregua di un "intermediario" del mondo virtuale. Le valute virtuali dei clienti vengono conservate su indirizzi della *blockchain* nella disponibilità esclusiva dell'*exchange*, unico soggetto in possesso delle relative chiavi crittografiche e in grado quindi di movimentarli; analogamente, la valuta fiat dei clienti viene conservata su rapporti, intestati all'*exchange*, accesi presso istituti bancari e/o finanziari (cfr. immagine). Per motivazioni operative volte alla gestione della contabilità della clientela, ad ogni cliente vengono associati uno o più indirizzi di "deposito", utilizzati per far confluire all'interno di uno specifico *wallet/account* disponibilità provenienti dall'esterno della piattaforma. Una volta accreditate le disponibilità su tali indirizzi di deposito, la piattaforma solitamente le trasferisce su altri indirizzi sotto il proprio controllo ovvero le usa per soddisfare le richieste di trasferimento verso indirizzi esterni che provengono anche da altri clienti. Secondo tale paradigma tecnologico, inoltre, solo le operazioni di trasferimento di valuta virtuale da/verso indirizzi "esterni" (cioè non gestiti dall'*exchange*) lasciano traccia all'interno della *blockchain*. Viceversa, le altre tipologie di operazioni (cambio cripto-fiat, cambio cripto-cripto e se previsto trasferimento tra *wallet* accesi dall'*exchange*) non lasciano alcuna traccia sul registro pubblico delle transazioni essendo trascritte esclusivamente nei sistemi gestionali dell'*exchange*.

Le conseguenze sull'analisi delle transazioni.

Le modalità di funzionamento degli *exchange* centralizzati hanno delle conseguenze sulla capacità di seguire i flussi in valuta virtuale mediante le strumentazioni tecniche disponibili in tale campo. Difatti, rispetto a un *wallet* gestito da un *exchange* centralizzato per conto di un proprio cliente, la tracciatura dei flussi mediante l'analisi delle transazioni in criptovaluta è possibile esclusivamente rispetto alle:

a) transazioni in ingresso; in tal caso le analisi mirano primariamente ad identificare gli indirizzi di origine delle disponibilità pervenute sul *wallet* e, nel caso questi siano a loro volta gestiti da altri operatori del comparto, ad attivare richieste volte ad ottenerne le relative movimentazioni nonché i dati acquisiti sui relativi titolari in sede di adeguata verifica;

di converso, le:

b) transazioni in uscita non sono generalmente univocamente identificabili in *blockchain* in quanto risultano "mescolate" rispetto a quelle degli altri clienti della piattaforma;
c) transazioni di cambio di valuta fiat da/ovvero in criptovaluta non vengono, come sopra accennato, affatto scritte in *blockchain*.

In ragione di ciò, tali due ultime tipologie di operazioni sono conosciute con certezza esclusivamente dall'*exchange* che gestisce il *wallet* e i relativi dati vanno quindi a quest'ultimo richiesti dalle autorità competenti (A.G., FIU etc).

Per tali considerazioni, nel caso in esame, l'unico profilo di approfondimento autonomo – cioè senza attivazione di richieste agli *exchange* coinvolti – delle transazioni in criptovaluta potrebbe riguardare l'**analisi delle transazioni in ingresso ai n. 3**

indirizzi riportati in premessa al fine di identificare ulteriori possibili flussi originati da altri *wallet* non noti.

Di seguito l'esito delle analisi condotte sugli indirizzi di interesse.

- Primo indirizzo *bitcoin*.

Alla luce delle informazioni il primo indirizzo, gestito da O, sarebbe stato accreditato mediante n. 85 operazioni di prelievo di *bitcoin* a valere di due *wallet* intestati a soggetti di interesse dell'indagine.

Si è quindi provato a confrontare tali operazioni con i dati disponibili in *blockchain*, reperiti mediante strumenti disponibili su fonti aperte[99], al fine di identificare ulteriori possibili transazioni in ingresso sull'indirizzo in parola.

A tal fine, rileva che il tracciato delle operazioni presente nella richiesta non riporta il riferimento univoco alle transazioni registrate nella *blockchain* (il c.d. *transaction hash*), per cui si è provato ad effettuare l'associazione tra l'operazione di prelievo e quelle registrate in *blockchain* confrontando la data e l'importo delle stesse. All'esito di tale analisi, sono state identificate, oltre alle 85 riportate nella richiesta, altre n. 8 transazioni per complessivi 20,9746 BTC, diverse delle quali sembrano provenire dall'*exchange* con sede in Lussemburgo.

Presso tale ultimo operatore potrebbe quindi essere presente un ulteriore *wallet* di possibile interesse per le indagini. Sfruttando inoltre strumenti di analisi delle transazioni in valuta virtuale si potrebbe provare a identificare l'entità che controlla gli indirizzi da cui provengono la restante parte delle transazioni (cfr. righe in grassetto).

- Secondo e terzo indirizzo *bitcoin*.

Su tali indirizzi, gestiti da H, alla luce delle informazioni disponibili nella richiesta, sarebbero pervenute da un *wallet* noto alle indagini complessive:

- n. 96 transazioni *Tether* (USDT).
- n. 28 transazioni *bitcoin*.

Rispetto alla sezione precedente, rileva che, nel caso dei due indirizzi in esame, sarebbero state perfezionate anche transazioni nella *stablecoin Tether* che, alla luce delle ricerche condotte su fonti aperte[100], può essere trasferita secondo diverse modalità, sfruttando anche diverse *blockchain*.

Nel caso in esame, sembrerebbe che il trasferimento si sarebbe perfezionato sfruttando la tecnologia offerta dalla piattaforma *Omni*[101] che, alla luce delle analisi effettuate su fonti aperte, è stata progettata per operare sopra la *blockchain* di *bitcoin* e consentire la creazione e lo scambio di *asset* digitali. I trasferimenti *Tether* che usano *Omni* sarebbero quindi registrati come transazioni della *blockchain bitcoin*. Tale ipotesi sembra trovare riscontro nelle ulteriori analisi condotte mediante lo strumento di analisi delle transazioni *Omni* identificato su fonti aperte[102] che ha consentito di identificare

99 Ad es. https://www.walletexplorer.com.
100 https://academy.binance.com/it/articles/what-is-tether-usdt.
101 http://www.omnilayer.org/.
102 https://omniexplorer.info/.

complessive n. 188 transazioni *Tether* in addebito e in accredito dei due indirizzi in esame. In assenza di uno strumento di *download* massivo di tali transazioni che avrebbe consentito un'analisi più puntuale delle stesse, l'analisi a campione condotta consente di stimare che queste transazioni siano sostanzialmente equamente suddivise tra operazioni in accredito e addebito. Alla luce di tali analisi qualitativa sembra quindi che la totalità o la quasi totalità delle transazioni Tether in ingresso siano identificabili con le operazioni di prelievo citate nella richiesta.

Per quanto concerne invece le transazioni in BTC, escludendo le verosimili transazioni Tether che sembrano siano comunque scritte nella *blockchain* di *bitcoin*, sono stati identificati n. 28 trasferimenti in ingresso ai due indirizzi in argomento, nella quasi totalità dei casi[103] sovrapponibili, secondo la logica delineata in precedenza, con quelli indicati nella richiesta.

Per le ragioni sopra espresse, non sembrano esservi, al di fuori di quelle già note nella richiesta, altre transazioni in ingresso sugli indirizzi *bitcoin* 1 e 2 sui quali potrebbero essere avviati ulteriori approfondimenti mediante strumenti di analisi forense delle valute virtuali.

In ragione degli elementi esposti, gli unici approfondimenti che sarebbe possibile condurre sulle transazioni in valuta virtuale senza richiedere la collaborazione di O e H, sfruttando strumenti di analisi forense delle valute virtuali, riguarderebbero le sole ulteriori operazioni in accredito sugli indirizzi oggetto di indagine originati da altri *wallet* (diverse delle quali tra l'altro già analizzate mediante strumenti disponibili su fonti aperte). L'analisi delle transazioni in criptovaluta "in uscita" da tali *wallet* con gli strumenti tecnologici in parola nonché di quelle di cambio da/ovvero valuta fiat richiede, invece, l'interessamento preliminare degli *exchange* in argomento.

5. Sequestri di criptovalute.

5.1. Panoramica delle questioni sul sequestro di bitcoin.

Nel contesto dell'imposizioni di vincoli su documenti digitali in generale, peculiari problematiche riguardano il caso in cui le autorità inquirenti procedano al sequestro o alla confisca di criptovalute.

Le criptovalute sono, come le prove digitali, caratterizzate dall'immaterialità e dall'essere dati informatici: sennonché la loro apprensione "fisica" è fortemente problematica in virtù della crittografia utilizzata per garantirne la sicurezza. Solo con la chiave privata è possibile "spendere" i *bitcoin*, ma il suo ritrovamento non è sufficiente a imporre sul *bitcoin wallet* un vincolo di indisponibilità. In realtà dovrebbero essere

103 In un caso è stata rilevata un'incongruenza tra le date di due operazioni caratterizzate comunque dal medesimo importo.

proprio le *chiavi private* ad essere oggetto di sequestro (o confisca), in quanto i *bitcoin* sono solo, sintetizzando all'estremo, delle trascrizioni sulla *blockchain.*

Una delle questioni che si pongono in riferimento alle chiavi private riguarda la disponibilità del *wallet*. Se esso è nella disponibilità non solo di un singolo soggetto ma anche degli *exchange* o dei *wallet providers,* le problematiche sono assimilabili a quelle del sequestro presso terzi.

Diversa questione riguarda l'effettiva titolarità di un *wallet* in assenza di una previa procedura di adeguata verifica effettuata da un *exchange* o da un *wallet providers*. Infatti, nessuno può dire con certezza che un determinato soggetto è "titolare" di un *address bitcoin* alla stregua di un conto corrente bancario; se più soggetti conoscono la chiave privata possono "spendere" i *bitcoin* in esso contenuti.

Il sequestro probatorio è quello che probabilmente comporta meno problemi nel caso di *bitcoin*. Come sappiamo, la *blockchain* delle criptovalute (ad eccezione di *Monero* e *ZCash*) è pubblica e trasparente, rendendo superfluo procedere all'"apprensione" dello storico delle transazioni per poterlo utilizzare in un procedimento. Basterebbe semplicemente consultare la *blockchain* (sul sito *internet https://www.blockchain.com/it/explorer* è possibile consultare ogni blocco aggiunto ed i precedenti, insieme alle transazioni in esso iscritte) e riprodurne il contenuto (ad esempio con una c.d. "*screen shot*" delle sole transazioni rilevanti e non dell'intera *blockchain*) acquisendo come prova documentale le transazioni in essa iscritta.

Riguardo il sequestro preventivo, questioni possono sorgere nel caso di sequestro delle chiavi private per poter assumere il controllo del *wallet*, effettuato presso i fornitori di servizi relativi alle criptovalute o sequestrando il computer di un soggetto privato. In tal modo, si mira a congelare i *bitcoin* per evitare che il "possessore" (*rectius*, l'individuo che ne conosce la chiave privata) possa servirsi di strumenti di *mixing* e far perdere le tracce sulla *blockchain* dei *bitcoin* posseduti. Per un'analisi più completa, bisognerebbe distinguere la tipologia di *wallet* da sequestrare, sempre se l'oggetto del sequestro viene considerata la chiave privata e non i dati informatici iscritti nella *blockchain*. Pur non potendo normalmente la chiave di accesso essere considerata equivalente al bene che si intende sequestrare nel caso del sequestro preventivo di criptovalute la conoscenza della chiave privata è l'essenza del *wallet* stesso, tanto che senza di essa i *bitcoin* rimarrebbero delle tracce sulla *blockchain* fini a sé stesse. Nel caso dei *wallet* "*online*", l'oggetto del sequestro dovrebbero essere i dati informatici salvati presso i *server* del *wallet provider* (o dell'*exchange*). Nel caso di portafogli "*desktop*", si potrebbe considerare oggetto del sequestro l'*hard disk* del *computer* dove è installato il *software* di gestione delle chiavi private. I c.d. "*paper wallet*", inoltre, sono portafogli dove la chiave pubblica e privata sono stampati su un foglio, pertanto in quel caso potrebbe bastare il sequestro del documento. Gli "*hardware-wallet*" sono invece dei dispositivi, in molti casi simili alle *pen-drive USB* che memorizzano e generano le chiavi private *offline*; in quest'ultima ipotesi dovrebbe eseguirsi il sequestro della *res* contenente le chiavi di decrittazione. Infine, con il termine "*brain-wallet*", si suole far riferimento al fatto che venga memorizzata da parte

di un individuo la chiave privata del proprio *wallet bitcoin*[104]. In tal caso non ci sarebbe nulla da sequestrare, integrando la situazione più complicata per congelare *bitcoin* o altre criptovalute.

Proseguendo, diverse sono le accortezze da adottare da parte degli investigatori nel procedere al sequestro di *bitcoin*. Innanzitutto, nel caso di *wallet software* o *online*, il sequestro dell'*hard disk* o il modificare la *password* del *wallet* non è misura sufficiente, in quanto l'utente può aver effettuato un *backup* dei dati o aver comunque la disponibilità della chiave privata. Bisognerebbe, pertanto, creare un nuovo indirizzo *bitcoin*, possibilmente utilizzando i c.d. "*cold-wallet*", ossia i generatori di chiavi private *offline*, decisamente migliori dal punto di vista della sicurezza. Successivamente, trasferire i *bitcoin* sequestrati presso il nuovo indirizzo. Di ciò è necessario redigere verbale, anche se la *blockchain* già di per sé testimonia i trasferimenti di criptovaluta in maniera affidabile e definitiva. In verità, sarebbe anche opportuno proteggere i *bitcoin* sequestrati da tentativi di sottrazione, ad esempio cifrando la chiave privata o adottando sistemi di *multisignature*. Oppure, per semplificare le operazioni, convertire i *bitcoin* in valuta avente corso legale, ma ciò può essere un'attività problematica in assenza in un quadro normativo che autorizzi l'operazione.

Concludendo, il tema del sequestro di *bitcoin* o di altre criptovalute può assumere aspetti polivalenti in base al caso concreto e alla tipologia di *wallet* utilizzato. In più, il relativo peculiare funzionamento richiede che gli investigatori adottino particolari cautele e misure.

5.2. L'esperienza fiorentina.

Anche in Italia si è proceduto al sequestro – seppure nell'ambito di una procedura civilistica – di una ingente quantità di *bitcoin* nei confronti dell'*exchange* di criptovalute denominato "*BitGrail*"; nel contesto di una procedura prefallimentare, seguita dalla sentenza di fallimento il Tribunale – che ha ritenuto configurabile una responsabilità civilistica della deposito irregolare – ha disposto il sequestro di circa 2.345 *bitcoin* e 4 milioni di Nano, e, nei confronti dell'amministratore, di circa 170 *bitcoin* e oltre 500.000 euro. I *bitcoin* sequestrati sono stati trasferiti su un indirizzo *bitcoin* creato appositamente per il curatore della procedura fallimentare. Le chiavi private del suddetto *wallet* sono state poi depositate in un luogo terzo e sicuro, di cui il curatore e il coadiutore o chiunque abbia preso parte al sequestro non è in possesso di copie, restando inoltre ignoto il luogo di relativa custodia. Ciò poiché era accaduto, durante la fase d'indagine del sito *web Silk Road*, che i due agenti dell'FBI che lavoravano al caso si

104 in realtà, più che memorizzare la chiave privata vengono memorizzate una serie di parole. Queste parole non vengono scelte a discrezionalità dell'utente, ma vengono individuate dopo aver trasformato la chiave privata in codice binario (applicando ad essa la funzione crittografica di *hash* SHA256), e associando ad ogni segmento di risultato ottenuto di codice una parola dal dizionario inglese in base alla sua posizione in ordine crescente. Per maggiori approfondimenti, si veda https://bitcoin-in-action.medium.com/seed-phrase-mnemonic-phrase-come-ottenerlo-e-come-ripristinarlo-b8f157331111.

fossero impossessati dei *bitcoin* sequestrati, essendo a conoscenza delle chiavi private dell'indirizzo su cui erano stati traferiti.

Si riportano in dettaglio le precauzioni adottate e le misure poste in essere per operare il sequestro delle criptovalute rimaste giacenti sulla piattaforma *BitGrail* (*bitcoin*, *Nano*, *Dogecoin*, *Litecoin*) nell'ambito del procedimento fallimentare, operazione difficile e complessa, anche perché non esistevano precedenti, per plurimi motivi.

Tratto da appunto tecnico della Polizia Postale: […]

"II semplice possesso delle chiavi private non garantisce il sequestro o congelamento dei fondi, poiché essi possono essere movimentati finché questi non vengono spostati dal proprietario che detiene certamente ancora copia della chiave o da chiunque ne sia a conoscenza. Allo stesso modo, rischi si corrono anche per quanto riguarda la generazione di nuovi indirizzi su cui versare le cifre sequestrate: per la delicatezza del protocollo, che in alcune implementazioni potrebbe non essere stato sviluppato correttamente e presentare errori, per la delicatezza della conservazione della chiave privata e altre problematiche connesse. In ultimo, vi è il rischio che anche una volta trasferito il corrispettivo in bitcoin*, questo vada in qualche modo perso o venga trasferito ulteriormente dall'indirizzo destinazione.*

Per questo motivo la Polizia Postale ed i periti nominati hanno progettato diverse soluzioni

attuative, chiamati protocolli, nessuno di questi preesistenti o consolidati, finalizzati proprio a rendere l'indirizzo di destinazione con le seguenti caratteristiche:

1. Sicuro — cioè indirizzo generato con numero pseudocasuale realmente unico e non noto a terzi che potrebbero prima o poi ottenere la stessa chiave privata e quindi disporre dei fondi indipendentemente dalla volontà dei periti e in modo totalmente anonimo;

2. Con chiavi multiple che possono anche essere note a chi ha operato il sequestro ma non sufficienti singolarmente a disporre dei fondi — la fuoriuscita delle criptomonete deve essere abilitata solamente in presenza di un numero di membri del team deciso a priori (es. almeno tre su cinque) cosi che nessuno sia in grado autonomamente di far fuoriuscire le criptomonete sequestrate e quindi ognuno singolarmente sia esente da responsabilità;

3. Funzionale al dissequestro — cioè sono stati testati gli indirizzi per verificare che fosse possibile, con le chiavi private generate e in mano ai periti, far in futuro fuoriuscire i fondi (es. in caso di dissequestro, confisca, etc.).

4. Riproducibile — bisogna essere in grado in qualunque momento e con strumentazione/software pubblicamente disponibili anche in futuro di accedere ai wallet creati o riprodurre l'operazione di creazione;

5. Estendibile — nel caso in cui una delle chiavi "di ridondanza" venga persa, è _necessario predisporre una procedura per generare nuovo wallet e trasferire nuovamente la criptomoneta.

Allo stesso modo, è stato ideato un protocollo da seguire rigorosamente per il trasferimento della criptomoneta posta sotto sequestro, che avesse queste caratteristiche:

l. Ove possibile, non renda mai disponibile ai periti la o le chiavi private che permettono l'uscita dei fondi dai wallet da sequestrare, cosi che la responsabilità di eventuali distrazioni di denaro da tali wallet non potesse in alcun modo essere ricondotta ai periti ma soltanto al soggetto proprietario di esso;

2. Permetta un trasferimento veloce ed efficace della criptomoneta dai wallet posti sotto sequestro a quelli generati dai periti che verranno messi a disposizione dell'Autorità Giudiziaria.

Per la creazione dei wallet sono state usate le seguenti modalità esecutive:

***Wallet multisig** — A grandi linee, il protocollo di creazione dei wallet su cui versare i fondi può essere il seguente, per ogni criptomoneta che fornisce la possibilità di generare wallet multisig (cioè con il vincolo che per spendere i fondi e necessaria la presenza di pia chiavi e quindi di più persone contemporanee):*

1 Decisione di quanti membri faranno parte del pool e di quanti saranno necessari per "sbloccare" i fondi in futuro in caso di dissequestro, in modo che il collegio peritale non sia autonomamente in grado di far fuoriuscire la criptomonete neanche con accordo dei tre periti ma sia comunque necessaria anche la presenza di Giudice o PM;

2. Accensione dei PC in ambiente sicuro, isolato (fuori da rete Internet), riproducibile, documentato, con utilizzo di software (sistema operative wallet, etc ... di cui e stata preventivamente verificata l'integrità);

3. Creazione delle singole chiavi, in modo che ogni membro sia in grado di vedere soltanto la propria;

4. Creazione del wallet destinazione e di un indirizzo di destinazione;

5. Spegnimento dei PC;

6. Trasferimento di una quantità di criptomoneta di test sull'indirizzo presente nel wallet generato ai punti precedenti e destinato a contenere la cifra sequestrata;

7. Accensione dei PC in ambiente sicuro, isolato, riproducibile, documentato;

8. Apertura del wallet con la partecipazione del minimo numero di membri necessari per poter disporre del contenuto; Trasferimento delta cifra di test verso indirizzo terzo (per verificareche sia possibile in futuro restituire i fondi o confiscarli);

9. Spegnimento dei PC;

10. Consegna delle chiavi in busta chiusa al Giudice.

***Exchange** — Per le criptomonete supportate da Exchange come bitcoin.de o TheRockTrading (istituzioni private ma riconosciute a livello governativo/fiscale/bancario) si ravvede in ogni caso la possibilità – su autorizzazione del Giudice – di predisporre un wallet presso un Exchange custode (che quindi mantiene i fondi al suo interno, prendendone possesso ma lasciandone la disponibilità al registrante) intestato al Curatore (o a un Funzionario delegato) presso le loro strutture e generare un indirizzo verso il quale eseguire il trasferimento dei fondi, descritto nei passaggi successivi.*

Per le coin per le quali non è disponibile il wallet multisig, verrà creato un wallet/indirizzo singlesig (cioè per il quale e sufficiente una singola chiave per disporre delta moneta) che verrà testato come per il wallet multisig (test di ricezione moneta e testi di fuoriuscita) ma la chiave privata sarà stampata su carta in duplice copia, imbustata e sigillata che verra consegnata all'Ufficio Reperti.

***Nano** — Per quanto riguarda la criptomoneta Nano – sulla quale sono attestati più fondi in assoluto – al momento è impossibile generare wallet multisignature, è stata richiesta questa funzionalità agli sviluppatori proprio a seguito delta nomina e gli sviluppatori hanno realizzato un sistema che ha permesso di creare portafogli condivisi.*

***Opendime** — La soluzione basata su hardware Opendime consiste nell'avvalersi di particolari pendrive USB prodotte dalla società statunitense CoinK.ite che permettono la*

generazione sicura d'indirizzi bitcoin (unica moneta supportata per adesso) mediante smartcart su chipset ATSAMD21E17. Gli indirizzi bitcoin vengono generati a partire da un file di contenuto casuale salvato su ogni pendrive opendime, che raggiunti i primi 256k di "entropia" generano un file contenente l'indirizzo bitcoin che sarà per sempre legato alla pendrive.

La chiave privata legata a tale indirizzo invece non potrà uscire ne essere visionata a meno che non si "rompa" il contatto interno alla pendrive, bucandone la struttura in un punto preciso tramite un piccolo oggetto appuntito.

Il vantaggio di queste pen-drive e che, una volta versati i bitcoin su di esse (o meglio, sugli indirizzi da esse generati) possono essere considerate in tutto e per tutto dei "contanti", cioè una risorsa che contiene all'interno i bitcoin (in realtà la chiave privata per trasferire i bitcoin).

Questo tipo di pen-drive sono utilizzate da tempo dalla comodità e non hanno presentato problemi di sorta, generano le chiavi in modo casuale e forniscono persino un sistema per la verifica della casualità degli indirizzi generati.

Poiché non è possibile generare backup o esportare le chiavi (così come invece avviene per i wallet hardware tradizionali come Trezor o Ledger) un eventuale danneggiamento alia pendrive implicherebbe la perdita dei fondi ivi attestati.

Per questo motivo si è ritenuto di dover suddividere l'importo sequestrato in una ventina di OpenDime, così da limitare l'eventuale rischio di rottura di un dispositivo.

Il vantaggio di questa soluzione invece è il fatto che non è possibile che il collegio possa tenere alcuna chiave, neanche in modalità condivisa/multisig, poiché le chiavi private non possono essere lette e quindi le pendrive stesse diventano la "chiave" di sblocco dei fondi, motive per il quale andranno poi depositate in luogo sicuro, essendo del tutto paragonabili a del contante.

6. La giurisdizione, con particolare riferimento al riciclaggio mediante criptovalute.

L'infrastruttura tecnologica delle criptovalute è allineata al desiderio di creare realtà senza controllo da parte dello Stato, in piena libertà e riservatezza; i principi ispiratori del protocollo *bitcoin* scaturiscono, in effetti, dai movimenti crittoanarchici che pongono al centro dell'interesse la *privacy* e l'assenza dell'ingerenza del potere statale. Per perseguire questo scopo vengono sfruttati i disallineamenti con le previsioni del diritto in stato di continua rincorsa rispetto alla rapida evoluzione degli strumenti tecnologici. Un approccio tradizionalista che miri a far confluire la duttile realtà tecnologica nelle categorie dogmatiche del diritto penale rischia di pervenire a risultati imprecisi.

Infatti, in generale i reati commessi mediate l'utilizzo di sistemi informatici presentano peculiari elementi oggettivi. Rispetto alla struttura del reato, la nozione di "atti", "azione" ed "evento" va calibrata sui crimini commessi nel *cyberspazio*, nel quale l'azione si sovrappone e si confonde con l'evento, tradizionalmente considerato dalla dottrina come «*risultato esteriore, nettamente distinto dall'atteggiamento muscolare del reo e definibile a prescindere da esso*»; l'individuo con la propria azione mette in moto un processo articolato in più "azioni" il cui risultato è difficilmente percepibile "naturalisticamente", mentre è arduo qualificare l'azione dell'uomo come attività di carattere esteriore, avendo effetti percepibili in senso logico-informatico (in forma di

codice binario). L'azione dell'individuo nella maggior parte dei casi non è quella descritta dal "fatto" del reato, ma sarà l'esecuzione automatica da parte dei sistemi informatici a rilevare per la tipicità della norma incriminatrice. Ciò determina anche che l'evento del reato perde la sua connotazione materiale, intesa come modificazione della realtà esteriore[105].

Inoltre, ulteriori problematiche sorgono in relazione all'applicazione spaziale della legge penale e al *tempus commissi delicti*.

La prima questione, la sua soluzione è rilevante per la determinazione della giurisdizione e competenza. Il cyberspazio non ubbidisce alla logica territoriale dei confini nazionali (per sua natura è infatti a-temporale), a differenza degli ordinamenti statali che richiedono uno «*spazio sul quale esercitare la propria sovranità esclusiva*»[106]. Inoltre, la rete permette la de-territorializzazione dell'individuo, che può agire ed essere presente in più "luoghi informatici", come anche la de-temporalizzazione delle azioni, ossia programmare e automatizzare complesse operazioni senza il necessario e simultaneo "contatto fisico" tra uomo e sistema informatico (si pensi alla realizzazione di *criminal smart contracts* dove è possibile pianificare a monte il *software*, la cui esecuzione causerà l'evento rilevante per la norma incriminatrice solo successivamente e al verificarsi di determinate condizioni previamente stabilite ed automaticamente eseguite). Smaterializzazione, velocizzazione, deterritorializzazione, ubiquità e de-temporalizzazione coinvolgono le condotte concrete che prescindono o di distanziano dalla fisicità dei comportamenti o dei fatti esteriori (ossia dall'azione o omissione tradizionalmente intese) capaci di incorporare l'accadimento materiale (il danno o il pericolo concreto).

Le norme del codice penale rilevanti in questo caso sono gli artt. 3 e 6, riguardanti l'obbligatorietà della legge penale e i reati commessi nel territorio dello Stato. L'art. 6 cit., in particolare, in ossequio al principio di territorialità, afferma che un soggetto viene punito in base alla legge penale italiana se ha commesso un reato nel territorio dello Stato (per la cui nozione cfr. artt. 3 e 4). Secondo una logica espansiva dell'applicazione

---

105 F. RUGGIERO, *Momento consumativo del reato e conflitti di giurisdizione nel* cyberspazio, in *Giurisprudenza di merito*, n. 1/2002, p. 255: «Sul piano tecnico, la Rete si pone come un articolato sistema di elaboratori elettronici in collegamento telematico, diffuso in tutto il mondo e capace di annullare qualsiasi distanza di tempo e di luogo, rendendo accessibili informazioni ad una sfera illimitata di persone in brevi scansioni cronologiche ed a basso costo. A differenza degli altri mass-media Internet presenta uno spazio di operatività geografica preventivamente non delimitabile, una struttura aperta ed uno sterminato numero di connessioni; mancando una forma di organizzazione gerarchica, la Rete risulta "anarchica", «acefala» e decentralizzata: si fonda, in definitiva, soltanto su un protocollo unitario relativo alla tecnica di trasferimento dei dati, che garantisce il collegamento a tutti i computers aderenti alla suddetta procedura».

106 S. SEMINARA, *Locus commissi delicti, giurisdizione e competenza del cyberspazio*, (relazione al Convegno "Presi nella rete – Analisi e contrasto della criminalità informatica", Pavia, 23 novembre 2012), osserva: «In particolare, al fine di inquadrare il tema della giurisdizione e della competenza in rapporto agli illeciti commessi per mezzo di Internet, occorre porre a raffronto due elementari constatazioni: la prima è che Internet ignora i confini territoriali e, dunque, la territorialità degli ordinamenti giuridici; la seconda è che gli ordinamenti giuridici necessitano invece di uno spazio sul quale esercitare la propria sovranità esclusiva e ulteriormente tendono ad allargare i propri confini applicativi sulla base di valutazioni legate alla qualità del soggetto attivo o del soggetto passivo o alla natura del reato commesso».

della legge penale italiana, il capoverso della disposizione, in omaggio al criterio dell'ubiquità, estende il *locus commissi delicti* anche a semplici frazioni dell'azione o dell'omissione nonché alla mera realizzazione dell'evento (Cass. VI, n. 26716/2003).

Per parte dell'azione o dell'omissione deve intendersi una frazione dell'azione "tipica", ossia del reato consumato o tentato. Perché si creino le condizioni per la punibilità in Italia non occorre, però, che la parte di azione od omissione ivi realizzata sia essenziale per l'integrazione del reato, ma è sufficiente che nel territorio nazionale sia stato *posto in essere anche uno solo degli atti del processo criminoso essenziali per la configurabilità del reato medesimo* (Cass. I, n. 2640/1995). Ai fini dell'affermazione della giurisdizione italiana in relazione a reati commessi in parte all'estero, *non* può essere riconosciuta rilevanza ad un *generico proposito*, privo di concretezza e specificità, di commettere all'estero fatti delittuosi, poi lì integralmente realizzati, sotto il profilo soggettivo e oggettivo (Cass. VI, n. 56953/2017).

L'evento richiamata dal capoverso dell'art. 6 è quello in senso naturalistico, ossia la modificazione del mondo esterno dipendente dalla condotta, e non l'evento in senso giuridico, cioè l'offesa arrecata dal fatto all'interesse tutelato. Infatti, se l'evento fosse inteso in senso giuridico, la previsione di cui all'art. 7, sulla punibilità dei reati commessi all'estero ma la cui offensività si realizza in Italia, diverrebbe superflua (si pensi, ad esempio, ai delitti previsti nei primi quattro numeri dell'art. 7, che sarebbero già punibili in forza dell'art. 6, comma 2). La dottrina più risalente riteneva che la soglia minima di condotta rilevante *ex* art. 6 cit. fosse data dal tentativo. Tuttavia, la dottrina più moderna e prevalente *non ritiene necessario il raggiungimento nel territorio dello Stato della soglia del tentativo*, perché, altrimenti, l'art. 6 diverrebbe superfluo, in quanto l'art. 56 già assicura la punizione degli atti idonei diretti in modo non equivoco a commettere un delitto realizzati in Italia. In questo senso è orientata anche la giurisprudenza, che ritiene *sufficiente a radicare la giurisdizione italiana la circostanza che sul territorio nazionale si sia verificata una parte della condotta, anche minima e consistente in frammenti privi dei requisiti di idoneità e inequivocità richiesti per il tentativo, purché preordinata al raggiungimento dell'obiettivo criminoso* (Cass. IV, n. 6376/2017). In caso di *concorso di persone*, data la struttura unitaria dell'istituto, si ritiene *applicabile la legge penale nazionale a tutti i compartecipi e a tutta l'attività criminosa, ovunque realizzata, quando in Italia sia stata posta in essere una qualsiasi attività di partecipazione ad opera di uno qualsiasi dei concorrenti*, a nulla rilevando che tale attività parziale non rivesta in sé carattere di illiceità, dovendo essa essere intesa come frammento di un unico iter delittuoso da considerarsi come inscindibile (Cass. III, n. 35165/2017). Per quanto riguarda la continuazione, l'unificazione dei reati per l'esecuzione di un medesimo disegno criminoso riguarda solamente alcuni effetti, quali la pena, ma *non incide sul luogo del commesso reat*o (Cass. VI, n. 25889/2006). Ne consegue che i vari episodi criminosi devono essere scissi in base alla loro realizzazione in Italia o all'estero. Pertanto, non potranno ritenersi punibili reati commessi interamente all'estero, sebbene in esecuzione del medesimo disegno criminoso. E ciò anche se tali reati commessi all'estero sono in continuazione con altri che risultano punibili ex art. 6. Potrà ritenersi sussistere continuazione tra i reati commessi in Italia ed i reati commessi in tutto o in parte all'estero solo qualora questi ultimi siano punibili in base alla legge italiana. In tema di reati associativi, per

determinare la sussistenza della giurisdizione italiana occorre verificare in quale luogo è divenuta concretamente operativa la struttura dell'associazione, potendosi attribuire importanza anche al luogo in cui sono stati realizzati i singoli delitti commessi in attuazione del programma criminoso, quando essi stessi rivelino, per il numero e la consistenza, il luogo di operatività della predetta struttura (Cass. VI, n. 10088/2011).

Ciò posto l'applicazione di tali regole ai reati implicanti l'impiego di criptovalute commessi con la rete internet non è scevra da dubbi. Fondamentale determinare quando un reato commesso mediante l'uso della rete *internet* sia considerato come commesso nel territorio italiano e quando chi lo commette possa essere considerato alla luce del codice come presente all'interno dei confini nazionali.

È arduo rispondere con certezza, considerando la struttura decentralizzata delle *blockchain*. Diverse sono le soluzioni prospettabili, poiché il registro dove vengono conservate le transazioni non è custodito in un solo luogo ma ubiquitario, ma ogni copia è conservata in ogni singolo nodo della rete, sparsi in tutto il pianeta. Probabilmente l'unico elemento che distingue un blocco dagli altri è il *miner* che ne ha permesso la concatenazione. Una soluzione potrebbe essere quella di considerare una transazione avvenuta nel luogo in cui il *miner* ha risolto l'indovinello crittografico e ha "agganciato" il blocco alla *blockchain*. Tale soluzione comporterebbe una perenne incertezza sul "dove" la transazione è stata aggiunta al registro. Inoltre, una transazione affinché venga considerata come stabilmente inserita in un blocco valido, sia necessario che vengano aggiunti successivamente ad esso più blocchi, circa sei; può capitare infatti in caso di *fork* che una transazione venga aggiunto in un blocco che poi, in virtù del principio della catena più lunga, diventi un blocco "orfano" con il conseguente confluire delle transazioni in coda per essere aggiunti ai nuovi blocchi (che verranno aggiunti al ramo della catena più lunga). Quindi può accadere che seppur una transazione viene inserita in un blocco valido "minato" da un *miner* situato in un determinato paese, si considererà come stabilmente inserita nella *blockchain* nel momento in cui un altro *miner* vada ad aggiungere il sesto blocco successivo. Inoltre, in tutto ciò vi è un lasso di tempo (circa ogni 10 minuti viene aggiunto un nuovo blocco), che crea così uno scollamento temporale tra quando il soggetto agente ha effettivamente trasmesso la transazione e quando la stessa venga considerata come avvenuta.

Un ostacolo alla verificazione del luogo geografico dell'individuo che trasmette la transazione al *miner* è l'utilizzo di VPN (*virtual private network*)[107] e di *browsers* con crittografia stratificata. Dal punto di vista informatico, anche se fisicamente il soggetto agente opera da un *computer* situato in Italia, risulterà come connesso a *server* ubicati in

[107] E. SIMONCINI, *Il* cyberlaundering*: la "nuova frontiera" del riciclaggio*, in *Riv. trim. dir. pen. econ.*, n. 4/2015, nota n. 53, p. 908: «Chiunque sia in possesso di un computer e di una connessione internet, può navigare in rete utilizzando il proprio indirizzo IP, ossia un indirizzo numerico che serve ad identificare e localizzare in maniera univoca ogni computer o dispositivo connesso ad una rete. Sebbene sia impossibile navigare senza un indirizzo IP, è possibile trovare nel web strumenti di navigazione che consentano di camuffare il proprio indirizzo IP, ottenendo un massimo livello di anonimato, in maniera tale che il proprio computer risulti collocato in un'altra città, in un altro Paese o, addirittura, in un altro continente (esempi sono rappresentati dai programmi *CyberGhost* VPN o *TunnelBear)*».

altri paesi, creando così difficoltà anche dal punto di vista probatorio e dell'effettiva applicazione della giurisdizione italiana.

Per quanto riguarda il *locus s*ed *il tempus comissi delicti* del delitto di riciclaggio, considerando che esso è un reato istantaneo, la soluzione preferibile sarebbe quella di considerare il luogo e il momento in cui il soggetto trasmette la transazione, in quanto, seppur di difficile accertamento per quanto detto, non rimane in balia della ubiquità del sistema di *mining* con tutte le sue insite incertezze sul luogo e tempo di iscrizione della transazione in un blocco. Inoltre, questa soluzione dovrebbe essere la più efficiente in termini di persecuzione del reato in quanto la giurisdizione sarebbe così affidata allo *stato in cui il soggetto agente fisicamente opera ed agisce*.

Nel caso degli *exchange*, che permettono scambio di criptovalute detenute tra gli utenti registrati alla piattaforma, o la conversione di valuta fiat con valuta virtuale, si potrebbe sostenere che il reato si consumi nel luogo dove essi hanno sede in quanto essi permettono e gestiscono le transazioni. Soluzione può risultare dubitabile ove si rimarchi che l'*exchange* opera solo come intermediario tra l'utente che desidera convertire la valuta in suo possesso e coloro i quali vorrebbero vendere le valute in loro possesso, venendo iscritta la transazione alla *blockchain* di *bitcoin* con le stesse modalità di qualsiasi altra transazione avvenuta senza l'intermediazione di terzi, ossia attraverso i *miners* e il meccanismo del consenso distribuito. Nel caso degli *exchange* centralizzati (v. *supra*), invece, i termini del controllo sulle criptovalute appaiono più qualificati ed orientano verso gestioni "territoriali" più nitide.

I.A., politica e reati contro la personalità dello Stato

di Claudio Orazio Onorati
Sostituto Procuratore presso il Tribunale di Napoli

SOMMARIO: 1. Obiettivi e metodologia. – 2. Area di ricerca. – 3. Atti di indirizzo e regolamentazione (UE ed extra UE) in tema di disinformazione tramite *social network*, *fake news* e *deep fakes*. – 4. Il fenomeno espansivo dei *deep fakes* e dei *social bots*. – 4.1. *Deep fakes*: definizione e funzionamento. – 4.2. Utilizzi illeciti e profili di rilevanza penale. – 4.3. Casistica. – 4.3.1. Pornografia. – 4.3.2. Interferenze in materia bancaria e finanziaria. – 4.3.3. Interferenze in ambito politico. – 4.3.4. Frode e spionaggio. – 4.4. Letteratura. – 4.5. Problemi emergenti e questioni da approfondire. – 5. Uso di I.A. in *cyber-war*, armi, terrorismo. – 5.1. *Weaponization* dell'I.A. – 5.1.1 Classificazione. – 5.1.2. Fenomenologia e possibili scenari. – 5.1.3. I.A. e armamenti bellici: le *smart weapons*. – 5.1.4. La risposta penalistica: problemi, limiti e prospettive. – 5.2. I.A. e *Law Enforcement*. – 5.2.1. Attività di indagine tramite I.A.: alcuni esempi concreti tratti dall'esperienza italiana. – 5.2.2. Criticità teoriche e pratiche. – 5.2.3. Principi per una possibile regolamentazione. – 6. Conclusioni e proposte.

1. Obiettivi e metodologia.

Scopo di questa prima parte del lavoro è stato l'inquadramento dei problemi giuridici e in particolare penalistici che, nella specifica area di competenza del gruppo (v. *infra*), si pongono sul duplice piano

a) dell'utilizzo dell'A.I. come strumento per il compimento di attività di rilievo criminale;
b) dell'utilizzo dell'A.I. come strumento di contrasto e di ricerca di prove rispetto ad attività criminali.

Il lavoro sin qui svolto si è articolato in tre momenti:

1) ricostruzione empirica dei fenomeni rilevanti;
2) raccolta, catalogazione e studio delle fonti di regolamentazione (ove presenti) e della letteratura in materia;
3) individuazione delle problematiche giuridiche emergenti.

2. Area di ricerca.

La ricerca si propone di indagare i seguenti ambiti tematici:

– **Disinformazione tramite internet** (***fake news***) finalizzata alla manipolazione dell'opinione pubblica, incitazione all'odio (*hate crimes*), sovversione dell'ordine democratico (es. *white supremacist*);

- **Creazione/manipolazione di immagini e video** (***deep fakes***) diffusi nella rete, per commettere o facilitare reati contro la personalità dello stato, terrorismo e reclutamento, interferenze elettorale; manipolazione del consenso, dell'autodeterminazione informativa e della libertà decisionale tramite *social bots* e la diffusione '*deep fake news*';
- ***Cyber-war*** e ***cyber-security***.

3. Atti di indirizzo e regolamentazione (UE ed extra UE) in tema di disinformazione tramite *social network*, *fake news* e *deep fakes*.

Regolamentazioni, raccomandazioni, reports e quadro giuridico di riferimento. Si tratta **prevalentemente** di documenti che si inquadrano nel **"soft law"**, tra cui spiccano:

A) Unione Europea.

- 2021: *Proposta di Regolamento del Parlamento Europeo e del Consiglio in materia di I.A.* ('Artificial Intelligence Act')[108], che prevede **obblighi minimi di trasparenza** nei confronti di creatori e **utilizzatori di *deep fakes***.

- 2020: *Joint report* di Europol, United Nations Interregional Crime and Justice Research Institute (UNICRI) and Trend Micro EC3 riguardante attuali e potenziali usi criminali di I.A. (*'Malicious uses and abuses of A.I.'*)[109]. Il focus è sui ***deep fakes*** **come emblema del potenziale criminale dell'uso improprio di I.A.**: a questo proposito, il report suggerisce alcune **modalità per limitare l'impatto sulla società della tecnologia dei *deep fakes*** attraverso la prevenzione, nuove regolamentazioni, campagne di *awareness* e la creazione di canali per riportare la presenza di *deep fakes* (es. *notice-and-takedown procedure*)

- 2019 Second report Interpol-UNICRI, '*Towards responsible A.I. innovation*' (*Report on Artificial Intelligence for Law Enforcement*). Segnalazione dei rischi connessi all'uso dei deep fakes per la commissione di reati

B) Stati Uniti d'America.

Una serie di nuove leggi è stata approvata in relazione a fenomeni specifici: interferenze elettorali e pornografia non consensuale.

[108] Cfr. https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52021PC0206.
[109] Cfr. https://www.europol.europa.eu/publications-documents/malicious-uses-and-abuses-of-artificial-intelligence.

- 2019: la California ha esteso il 'Truth in Political Advertising Act', Californian Elections Code part. 20010, per ricomprendere anche l'uso improprio di *deep fakes* nelle campagne elettorali.

- 2019: la California ha esteso la 'revenge porn' law includendo i *deep fakes* come possibili strumenti per commettere il reato.

- 2019: Virginia ha esteso la 'revenge porn' law, includendo i *deep fakes* come possibili strumenti per commettere il reato.

- 2019: il Texas ha introdotto una specifica fattispecie di reato (*criminal offense*) riguardante la condotta di fabbricazione di un video falso (*deep fake*) con l'intento di ingannare e influenzare il risultato delle elezioni.

- 2019: USA BILL '*Deep fakes accountability act*'.

- 2018: USA BILL ha emendato il titolo 18, *United States Code*, proibendo la diffusione di materiale audiovisivo fraudolento.

- 2019: USA *National Defense Authorization Act*: Report sulla tecnologia *deep fake*, e sulla *weaponization* dei *deep fakes* da parte di attori e stati stranieri.

C) Cina.

- 2019: la Cina ha dichiarato l'introduzione di nuove regolamentazioni riguardanti materiale video e audio distribuito online, incluse un divieto di pubblicare e distribuire i *deep fakes* con l'intento di ingannare gli altri utenti.

- 2020: diventa reato caricare online *deep fakes* o altre informazioni create con il tramite di intelligenza artificiale senza averlo comunicato espressamente.

D) Italia.

- 2020: **vademecum del Garante della privacy** sul fenomeno dei *deep fakes*[110].

[110] Cfr. https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9512278.

4. Il fenomeno espansivo dei *deep fakes* e dei *social bots*.

4.1. Deep fakes: definizione e funzionamento.

Il termine *deep fakes*, derivante dalla crasi delle parole '*deep learning*' e '*fake media*', indica immagini e video generati attraverso elaborati algoritmi di I.A., in grado di creare contenuti digitali falsi estremamente realistici[111].

I deep fakes si distinguono dai c.d. *cheap fakes* o *cheap fellows*, che invece sono falsi facilmente riconoscibili, anche ad occhio nudo.

Tra gli strumenti di I.A. più avanzati di creazione dei *deep fakes*, ci sono i GANs (Generative Adversarial Networks), inventati nel 2014 dal ricercatore Ian Goodfellow e altri ricercatori dell'università di Montreal[112]. I GANs funzionano in base alla teoria del gioco: due Artificial Neural Networks competono l'uno contro l'altro. Il primo crea il contenuto falso, attraverso l'elaborazione di dati, il secondo testa se il contenuto è reale o creato dal software. Il primo migliora, finché il secondo non è più in grado di distinguere il vero dal falso[113].

I *deep fakes* hanno raggiunto l'attenzione pubblica e dei media nel 2017, quando su alcune *community* del sito 'Reddit' sono stati pubblicati falsi filmati pornografici di attrici e cantanti, delle quali è facile reperire immagini e dati essenziali per l'elaborazione del falso. Grazie a internet e ai social media, la tecnologia può raggiungere milioni di persone in tutto il mondo in pochi secondi e senza confini.

Ambito di applicazione lecita dei *deep fakes* riguardano il mondo del cinema e dell'animazione, l'arte e l'intrattenimento in generale, avatar virtuali che agiscono parlando numerose lingue ecc.

Per identificare i *deep fakes* è spesso necessario l'utilizzo di speculari algoritmi di A.I., che *in via automatica* sono in grado di intercettare i falsi. Negli ultimi anni sono proliferati studi scientifici su come identificare e combattere i *deep fakes*, molti di questi supportati da grandi aziende del digitale, social media *platform* e motori di ricerca – come Facebook, Google, Microsoft, Skype, Twitter – ove i *deep fakes* trovano diffusione. Queste *tech companies* stanno già elaborando algoritmi I.A., sistemi per le segnalazioni da parte degli utenti, e stanno formando team specializzati nel monitoraggio e contrasto al fenomeno della disinformazione. Sul punto, giova riportare la '*Deepfake Facebook detection challenge*' (DFDC) lanciata da Facebook nel 2019 al fine di accelerare lo sviluppo di nuovi modi per individuare i *deep fakes* video. La *challenge* ha riunito esperti, leader e accademici da tutto il mondo per sperimentare i loro modelli di *detection* e provare nuovi

---

[111] Definizione rinvenibile su https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9512278.

[112] R. CHESNEY – D.K. CITRON, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security* (2019) 107 California Law Review 1753, 1760; I.J. GOODFELLOW ET AL., *Generative Adversarial Networks* (2014) arXiv:1406.2661.

[113] *Ibidem*.

approcci. Ci sono numerosi studi di modelli, algoritmi e sistemi volti a riconoscere i *deep fakes*[114].

Nel 2020, Facebook ha elaborato una nuova policy riguardante i media manipolati e i *deep fakes*, che prevede la rimozione dal social dei *deep fakes* creati in modo di far credere ad una persona media che il protagonista del video e/o dell'immagine abbia detto o fatto cose che non ha mai detto o fatto. Dalla nuova policy sono esclusi immagini/video creati come parodia e satira[115].

Simili policy sui media manipolati sono state introdotte da Twitter[116] e da YouTube[117].

4.2. Utilizzi illeciti e profili di rilevanza penale.

L'impiego dei *deep fakes* può essere associato a una varietà di manifestazioni illecite[118], corrispondenti anche nel nostro ordinamento a diverse fattispecie penali.

Si segnalano in particolare

- Campagne di disinformazione globale ('*deep fake news*') e manipolazione dell'opinione pubblica, anche in ambito elettorale e in ambito sanitario e scientifico (campagne no-vax, false informazioni su Covid-19);
- Condizionamento dell'opinione pubblica su singoli attori politici o contro di essi;
- Pornografia non consensuale, *revenge porn*, pedopornografia;
- Diffamazione e *harassment* online;
- Fenomeni di *astroturfing*;
- Estorsione (es. minaccia di rilasciare un video falso che danneggerebbe la reputazione o la credibilità di una persona fisica o giuridica);
- Frodi;
- Falsi personali (sostituzione di persone e fenomeno di '*morphing attack*') e documentali (fabbricazione o alterazione di prove digitali in ambito processuale);
- Distorsione e manipolazione dei mercati[119] (es. diffusione di video falso in cui il CEO di una società quotata commette un reato o si lascia andare a commenti razzisti/misogini);
- Incitazione agli atti di violenza contro minoranze;

---

[114] Un esempio di studio può leggersi a questo link: https://arxiv.org/abs/2006.07397?fbclid=IwAR1n3A8Gr1Ldo8ojXw6ggzX0cCKOHKLD-jri5ZEHCSCJKNi4xoXaZCiqkNQ

[115] A. HOLMES, *Facebook just banned deepfakes, but the policy has loopholes – and a widely circulated deepfake of Mark Zuckerberg is allowed to stay up*, (Jan. 7, 2020) *Insider*: https://www.businessinsider.com/facebook-just-banned-deepfakes-but-the-policy-has-loopholes-2020-1?IR=T.

[116] https://blog.youtube/news-and-events/how-youtube-supports-elections.

[117] https://help.twitter.com/en/rules-and-policies/manipulated-media.

[118] 2020 Joint report di Europol, United Nations Interregional Crime and Justice Research Institute (UNICRI) and Trend Micro EC3 riguardante attuali e potenziali usi criminali di I.A. 'Malicious uses and abuses of A.I.', p. 52.

[119] Sul tema cfr. nello specifico J. BATEMAN, *Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios*, July 2020.

- Sostegno alla narrazione di gruppi estremisti o anche terroristici: forme più o meno subdole di indottrinamento o proselitismo
- Incentivo all'agitazione sociale e alla polarizzazione politica (es. teorie e cospirazioni) anche per finalità discriminatorie ai danni di gruppi sociali specifici o di natura sessualmente orientata.

4.3. Casistica.

4.3.1. Pornografia.

- Nel settembre 2019 la società di I.A. '*Deep Trace*' ha pubblicato uno studio dal quale emergeva che su 15.000 video di *deep fakes* diffusi *online*, il 96% era pornografico e il 99% di questi riguardava donne, famose, tramutate in pornostar.
- Ad oggi, dalla stessa documentazione esaminata, sono riportati pochissimi casi di utilizzo illecito di *deep fakes* in ambito diverso da quello della pornografia involontaria (revenge porn, ecc.).

4.3.2. Interferenze in materia bancaria e finanziaria.

- Nel 2014, in Bulgaria il governo ha accusato parti non specificate di coordinare un "attacco criminale" alla reputazione di diverse banche che avevano subito scalate e oscillazioni in borsa. L'episodio ha coinvolto messaggi di testo, post su Internet e fughe di notizie, alcune fattuali, altre contestate.
- Il 23 aprile 2013, un gruppo di hacker chiamato Syrian Electronic Army ha dirottato l'account Twitter dell'Associated Press e poi ha twittato: "*Breaking: Two Explosions in the White House and Barack Obama is injured*". Questa falsa affermazione ha scatenato un diluvio istantaneo di trading, che E-Trade ha definito "i due minuti più attivi nella storia del mercato azionario". Gli algoritmi di trading automatizzati hanno guidato gran parte del volume. In soli tre minuti, l'indice S&P 500 ha perso 136 miliardi di dollari di valore, e anche i prezzi del greggio e i rendimenti obbligazionari Treasury sono scesi.

4.3.3. Interferenze in ambito politico.

- ***Accelerazione della crisi politica in Gabon nel 2018***. Alla fine del 2018 fu postato in rete dal Governo locale un video del Presidente Bongo che rilasciava i tradizionali auguri per il nuovo anno. Il Presidente, che era stato assente per molti mesi dalla vita politica, era oggetto di una intensa speculazione politica sul suo reale stato di salute. Tuttavia, l'insolita apparizione di Bongo nel video ha portato molti sui social media, incluso il politico gabonese Bruno Moubamba, a dichiarare che il video era un *deep fake*, confermando il loro sospetto che il governo stesse coprendo la cattiva salute o la morte di Bongo. Una settimana dopo la pubblicazione del video tra crescenti disordini, i

membri dell'esercito del Gabon hanno lanciato un tentativo di colpo di stato, richiamando proprio la pubblicazione del video. Da analisi forensi non sono però emerse tracce che provino che fosse *deep fake* ed è emerso che da agosto 2018 il presidente aveva subito un grave ictus[120].

- ***Scandalo sessuale in Malesia nel giugno 2019***. Uno scandalo politico è emerso nel giugno 2019 intorno a un *sex tape* che coinvolgeva presumibilmente il ministro malese degli affari economici Azmin Ali e l'assistente maschile di un ministro rivale. Mentre l'assistente ha affermato che il video era reale ed è stato successivamente arrestato, Ali e i suoi sostenitori, incluso il primo ministro malese, hanno sostenuto che il video era un *deep fake* realistico fatto per sabotare la sua carriera politica. Tuttavia, gli esperti internazionali non sono riusciti a trovare alcun segno che il video fosse stato manipolato. A metà agosto 2019, non era ancora chiaro se il video sia originale o falso.

- ***Manipolazione audio della voce di Nancy Pelosi con uno 'shallow fake':*** a marzo 2019 fu pubblicato in rete un video, poi risultato manipolato. Nel video, che è stato condiviso il 23 maggio 2019, il discorso di Pelosi era stato rallentato, facendo sembrare che stesse biascicando le sue parole. La versione modificata del video è diventata virale sui social media ed è stata ritwittata dall'account Twitter ufficiale del presidente degli Stati Uniti Donald Trump, ricevendo oltre 6,3 milioni di visualizzazioni al 31 luglio 2019. Su una popolare pagina Facebook, il video ha ricevuto oltre 2,2 milioni di visualizzazioni nelle 48 ore successive al suo caricamento iniziale, con i commentatori che hanno definito Pelosi "ubriaca" e un "pasticcio balbettante"[121].

- ***Manipolazione di movimenti del corpo per la revoca del pass alla Casa Bianca del giornalista CNN Jim Acosta***. Un video *shallow fake* è stato anche citato come prova per giustificare azioni politiche controverse. In questo caso, il corrispondente della CNN Jim Acosta si è visto revocare il suo pass stampa alla Casa Bianca il 7 novembre 2018, a seguito della diffusione di un video in cui si mostra un membro dello staff della Casa Bianca che tentato di togliergli il microfono dopo uno scambio teso con il Presidente Trump

- ***Disinformazione nella pandemia di Covid-19***: secondo i report di Avast (marzo 2020) i rapporti di intelligence indicano principalmente la Russia e la Cina come i principali attori nell'avvio delle campagne di disinformazione. L'influenza russa in particolare ha raggiunto l'attenzione mondiale con Reuters (Emmott 2020), Guardian (2020) e Deutsche

---

[120] A. BRELAND, *The Bizarre and Terrifying Case of the "Deepfake" Video that Helped Bring an African Nation to the Brink*, Mother Jones, 15 marzo 2019; J. BLAKKARLY, *A gay sex tape is threatening to end the political careers of two men in Malaysia*, SBS News, 17 giugno 2019.

[121] S. MERVOSH, *Distorted Videos of Nancy Pelosi Spread on Facebook and Twitter, Helped by Trump*, The New York Times, 24 maggio 2019; C. MONJE JR., *Twitter letter to Chairman Schiff*, Twitter, 31 luglio 2019; D. HARWELL, '*Sexist' videos edited to make Nancy Pelosi look drunk go viral, with Trump's help*, The Independent, 24 maggio 2019.

Welle (2020) – tra gli altri – che coprono le notizie sostenute dalle fonti interne dell'UE. Creato dal Servizio europeo per l'azione esterna, il braccio di politica estera dell'UE, il documento afferma che la Russia sta servendo il suo obiettivo finale di sovvertire le società europee spingendo la disinformazione online in inglese, spagnolo, tedesco e francese sul virus al fine di confondere e ostacolare la risposta dell'UE alla pandemia. La campagna include informazioni contraddittorie e notizie false come l'idea che il virus sia un'arma biologica statunitense (Avast 2020). A sua volta la Cina rilancia tali false notizie anche mediante A.I. facendo emergere inadeguatezze degli USA nella gestione della pandemia e dei vaccini anche in contesti strategici come Taiwan.

- ***Attacchi via Twitter nei confronti del Presidente della Repubblica italiana in occasione della formazione del Governo dopo le elezioni politiche del 2018***. È attualmente in corso un'indagine per chiarire le dinamiche dietro la creazione, nella notte tra il 27 e il 28 maggio 2018, di circa 400 account Twitter utilizzati per condizionare l'opinione pubblica e favorire le dimissioni del Presidente della Repubblica Sergio Mattarella a seguita del suo rifiuto della proposta del Presidente del Consiglio incaricato, Giuseppe Conte, di nominare Paolo Savona Ministro dell'Economia. È stata condotta un'analisi degli account che hanno rilanciato tweet con hashtag diventati virali – #mattarelladimettiti, #impeachment e #impeachmentmattarella – per individuare eventuali *bot*. Quali criteri sono stati utilizzati la composizione dello username e le informazioni pubbliche di base del profilo; il rapporto tra numero di following e followers; i collegamenti tra following e followers; i temi trattati nei tweet. Come risultato sono emersi sopracitati 360 account "anomali" di cui si può ritenere plausibile che, per la loro creazione e contestualizzazione nel brevissimo tempo in cui sono emersi, siano stati utilizzati particolari algoritmi basati sull'intelligenza artificiale.

4.3.4. Frode e spionaggio.

- ***Account LinkedIn di Katie Jones***. Uno studio di Deep Trace documento che nel 2019 è stato scoperto un account LinkedIn, registrato sotto il nome di Katie Jones, che si presentava come collaboratrice di un *think tank* statunitense. L'account ha effettuato 52 connessioni, tra cui membri del personale dei funzionari governativi. L'analisi di vari esperti ha individuato diverse anomalie visive indicative del fatto che l'immagine era stata generata artificialmente. L'account è stato rapidamente rimosso di LinkedIn.

- ***Account Twitter di Maisy Kinsley***. Nel marzo 2019 è stato attivato che appariva e si presentava (anche con foto) come l'account Twitter di una "senior journalist", Maisy Kinsley, ha inizio a seguire vari *trader* dell'azienda Tesla ed è stato oggetto di denuncia da parte dell'azienda per tentativi di carpire dati personali e riservati; le indagini hanno svelato che vi erano diverse anomalie.

4.4. Letteratura.

Il primo approfondito lavoro sulle conseguenze e i pericoli connessi ai *deep fakes* è di Chesney and Citron[122]. Gli autori distinguono tra i danni che i *deep fakes* possono causare agli individui da quelli che possono produrre su larga scala all'intera società, e delineano delle possibili soluzioni di natura tecnologica, legale e finanziarie.

La maggior parte della letteratura è statunitense e riguarda la pornografia e l'interferenza elettorale.

Da una angolatura non penalistica, un nutrito filone analizza l'impatto della disinformazione sulla società moderna, sull'ordine pubblico e sulla democrazia, nonché il ruolo delle compagnie private nell'individuazione e rimozione dei *deep fakes*.

Non risulta invece letteratura concernente specificamente il tema dell'uso dei *deep fakes* in ambito terroristico o di criminalità organizzata.

4.5. Problemi emergenti e questioni da approfondire.

- *Gap* normativo nazionale sia a livello di diritto sostanziale che a livello processuale. Si rende necessaria una analisi delle fattispecie incriminatrici vigenti per verificare i margini di effettiva applicabilità a fronte dei fenomeni in esame. La lacuna normativa può generare gravi impunità, nonché rischi per la collettività, tenuto conto che la criminalità organizzata e i gruppi terroristici possano trovare nuovi campi d'azione nel *cyberspace* utilizzando gli strumenti di manipolazione di consenso e di informazione, senza confini e limiti. Un obiettivo è reperire casistica giudiziaria rilevante rispetto allo scopo del nostro gruppo. È verosimile ipotizzare la necessità di introdurre nuove fattispecie ed aggravanti.

- È necessaria una riflessione, a monte, sul tipo di approccio che l'ordinamento dovrebbe adottare nei confronti di questi fenomeni. In particolare, si tratta di scegliere, o meglio di individuare un punto di equilibrio, tra prevenzione e criminalizzazione di condotte ad oggi lecite.

- È importante analizzare come individuare e bloccare questi fenomeni di criminalità organizzata alla luce della 'deregulation' e del ruolo dei privati, che sono fornitori di strumenti di 'detection' dei deep fakes (*startup* e *tech companies* nel campo dell'I.A. che producono *deep fakes* e *anti-deep fakes tools*), ad oggi indispensabili per intercettare e riconoscere i *deep fakes*.

- Ruolo di Interpol ed Europol nell'uso di I.A. per la commissione di reati.

[122] R. CHESNEY – D.K. CITRON, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 California Law Review 1753 (October 15, 2019).

- Proposta di regolamento Commissione Europea (A.I. Act). La proposta ha lo scopo principale di controllare, migliorare e sviluppare lo sviluppo del mercato dell'I.A., cercando ridurre il più possibile le forme di limitazione, prediligendo la strada del potere di controllo del mercato della Commissione. È adeguata la soluzione proposta per il problema dei *deep fakes*? Ovvero la loro identificazione come sistemi a rischio medio e la sottoposizione al loro uso e diffusione a meri obblighi di trasparenza? È necessaria una comparazione con l'approccio statunitense e con quello cinese.

- Problemi di giurisdizione legati alla natura transnazionale del fenomeno. Necessaria un'armonizzazione della materia a livello sovranazionale, si pensi alla necessità di reperire informazioni tramite strumenti di cooperazione giudiziaria, in quanto autori e algoritmi dei *deep fakes* possono essere virtualmente collocati in un paese dove il fenomeno non è criminalizzato.

5. Uso di I.A. in cyber-war, armi, terrorismo.

È soprattutto in questa materia che è emersa la tendenza degli studiosi – sia nei sistemi di common law che a livello europeo – a esaminare i problemi concernenti l'I.A. sotto due profili distinti:
1) **la "*weaponization*" dell'I.A.** che grazie a nuovi software e alla globalizzazione della rete potrebbe essere "istruita" in modo deviato allo scopo di realizzare attentati, da parte di gruppi terroristici; in quest'area rientra, anche se più limitatamente, l'uso di droni e macchine robotiche come armi schierate sul campo di battaglia;
2) l'utilizzo dell'intelligenza artificiale come **strumento di *law enforcement*** per analizzare enormi quantità di dati, nel mondo e nella rete, allo scopo di vedere interrelazioni tra soggetti ed eventi e indagare, contrastare o anticipare attentati ed eventi terroristici.

5.1. Weaponization *dell'I.A.*

5.1.1 Classificazione.

Molti documenti, ripresi di recente anche dal rapporto UNICRI di maggio 2021[123], ipotizzano tre scenari di utilizzo distorto dell'A.I.:

1) utilizzo concreto di nuovi algoritmi nocivi per condurre e portare a termine (massimizzando) un attacco;

[123] http://www.unicri.it/News/Algorithms-Terrorism-Malicious-Use-Artificial-Intelligence-Terrorist-Purposes

2) interventi per distorcere il funzionamento degli algoritmi esistenti allo scopo di "deviarne" le azioni e le risposte in modo coerente con le finalità terroristiche: in pratica, dunque, il principio è quello dell'attacco informatico che potrebbe modificare (rendendole fallaci, invertendo anche la loro utilità) alcuni sistemi informatici e di A.I.. Questo, secondo l'UNICRI è il tema del futuro, a causa dell'utilizzo sempre più esteso di Intelligenza artificiale;
3) stando al quadro ricostruito dall'agenzia dell'ONU, il primo riferimento concreto (e di cui è stato già confermato l'uso) è l'utilizzo di macchine totalmente automatizzate come i droni. I terroristi, infatti, hanno già utilizzato questi mezzi per effettuare ricognizioni aeree e localizzare i punti sensibili in cui portare avanti i propri attacchi;
4) l'utilizzo delle nuove tecniche di "*brain-reading*" già utilizzate per curare effetti di malattie neurodegenerative potrebbero essere trasferite in un A.I. allo scopo di instillare, incertezza, sfiducia, paura e rabbia in gruppi o collettività agendo sulla sicurezza psicologica, ed utilizzate a scopi terroristici.

5.1.2. Fenomenologia e possibili scenari.

L'impiego nocivo dell'I.A. (MUA.I.: "Malicious Use of Artificial Intelligence" [124]), specie per finalità terroristiche, può concretizzarsi in numerosi modi.

- Sabotaggio dei sistemi integrati e onnicomprensivi di I.A. (es. infrastrutture, sistemi di trasporto robotici ad autoapprendimento con gestione centralizzata basata sulla I.A.), preziosi obiettivi per atti di destabilizzazione;
- Ri-orientamento ad opera del terrorismo dei sistemi commerciali di I.A. e creazione di *deep fake* (vocali e visive) che possono colpire bersagli simbolici – tipicamente, leader politici e personaggi carismatici, ovvero icone culturali, religiose e centri di poteri;
- Condizionamento di campagne politiche, manipolazione di future elezioni e della politica globale, pregiudicando la stabilità geopolitica e creando un clima psicologico propizio per il successo di ulteriori azioni ostili;
- Creazione ed utilizzo di armi prognostiche – cioè metodi di analisi predittivi basati sulla I.A. e sui *big data*, che consentono di predire il futuro (disordini civili, epidemie, crisi economiche, risultati elettorali, ecc.) – a detrimento dell'avversario.
- Utilizzo di algoritmi in combinazione con stampanti 3D per la stampa di armi: nel settore delle armi leggere esistono diverse organizzazioni che mettono a disposizione online in *open source* modelli digitali di armi in file CAD che possono essere scaricati e stampati in 3D.

Ancora, il rapporto UNICRI di maggio 2021[125] prospetta varie tipologie di attacco:

[124] Cfr. BRUNDAGE ET AL., 2008, per l'espressione "*Malicious Use of Artificial Intelligence*" – MUA.I., e per il significato che gli autori attribuiscono a "*malicious*" ("We define "malicious use" loosely, to include all practices that are intended to compromise the security of individuals, groups, or a society": p. 9.).

[125] http://www.unicri.it/News/Algorithms-Terrorism-Malicious-Use-Artificial-Intelligence-Terrorist-Purposes.

- utilizzo di I.A. come una maniera per potenziare capacità *cyber* o permettere attacchi fisici veri e propri che sfruttino vulnerabilità e manomissioni di dati e sistemi (attacchi DDos con *machine learning* sono stati condotti dall'ISIS), con l'effetto di paralizzare intere città o infrastrutture strategiche;
- attacchi fisici attraverso la manipolazione di sistemi di guida autonoma di auto o di droni (per facilitare attacchi o per causare direttamente incidenti), o tramite interventi di *data poisoning* (per alterare i segnali di input o la loro lettura) sui sistemi di navigazione a guida elettronica di navi e aerei per massimizzare effetti di attacchi o rallentare soccorsi;
- utilizzo di I.A. per eludere i sistemi di controllo automatizzati e così recuperare fondi, facilitare propaganda e disinformazione, attuare tecniche di *social engineering* o rubare identità e falsificare passaporti (specie muovendosi nel *dark web*)
- utilizzo programmato di droni, sia a fini di sorveglianza che di attacco, sfruttando il fatto che non dispongono dei sistemi di sicurezza esistenti per le auto.

Le tipologie di attacco elencate nel rapporto possono essere distinte fra minacce che prevedono l'utilizzo dell'I.A. e minacce che, diversamente, ne realizzano un abuso. Nel primo caso si tratta di attori che impiegano direttamente tecnologie legate all'intelligenza artificiale per effettuare attacchi o massimizzarne l'efficacia, mentre nel caso di abuso si tratta di attacchi all'operatività o funzionalità di un sistema di intelligenza artificiale manipolato mediante tecniche *cyber* o cinetiche.

5.1.3. I.A. e armamenti bellici: le *smart weapons*.

Il livello di sicurezza delle operazioni di *intelligence* e militari relative a *cyber*-attacchi non consente di avere a disposizione documentazione recente.

Esistono però alcuni articoli dedicati a sistemi di armamento autonomo[126], quali droni impiegati per attacchi nella guerra all'ISIS e sottomarini a guida autonoma utilizzati in America Centrale dai cartelli del narcotraffico per sfuggire ai controlli.

Tra i sistemi di armamento noti, i principali esempi sono:

- sviluppo da parte degli USA del sistema antimissile e antiaereo THAAD;
- il progetto *Perdix*, che consiste nell'utilizzo di sciami di 20 o più droni armati che operano in formazione per svolgere un determinato compito; in Germania è stato sperimentato analogo sistema;
- sistema missilistico autonomo *Brimstone* sviluppato per la Royal Air Force (Regno Unito). Si tratta di un missile progettato per ingaggiare bersagli terrestri e piccole imbarcazioni, che può funzionare in modalità *fire and forget*. Infatti, in questa modalità, il software all'interno del missile cerca un bersaglio predeterminato all'interno di una zona definita *kill box*. Una volta che il software riconosce un bersaglio, ordina al missile

[126] Per l'elenco completo cfr. Intelligenza artificiale e armi autonome, in Mondo Internazionale Post, 5 giugno 2020; A. LELE, *Disruptive Technologies for the Militaries and Security*, Springer, 2019; Paul SCHARRE, *Army of None: Autonomous weapons and the future of war*, W.W. Norton&Company, 2018.

di colpirlo. Secondo quanto riferito, il *Brimstone* è stato usato contro obiettivi dello Stato islamico in Siria;

- mini-carrarmati guidati da remoto (per quanto riguarda la Russia). Il veicolo senza pilota si chiama Uran-96 ed è equipaggiato con una torretta mitragliatrice, un lanciafiamme e un'arma anti-carro. Ha già sviluppato elicotteri a guida totalmente autonoma e sperimentato l'uso, diretto da remoto, di robot "killer" che attaccano da soli, senza alcun intervento umano, obiettivi autonomamente selezionati in base a parametri preimpostati.
- robot totalmente automatizzati, autoveicoli militari a guida autonoma, droni anti-radiazioni che cercano, individuano ed attaccano i centri radar nemici senza alcun controllo e supervisione umana (Israele). Nel carrarmato Merkava IV Israeliano sono stati anche installati sistemi automatici di scoperta e soppressione del fuoco; Israele ha anche annunciato la creazione del primo blindato a guida autonoma in grado anche di recuperare e trasportare feriti (progetto Carmel).

Si prevede inoltre che molto presto saranno disponibili per l'impiego in scenari operativi:

- robot militari, non ricalcanti sempre le fattezze umane, ma autonomi e dotati di capacità decisionale. I prototipi in fase di sviluppo sono di vario genere: robot da trasporto (in grado di spostare carichi di centinaia di chilogrammi), da ricognizione (in grado di raggiungere velocità di quasi 50 km/h e saltare ostacoli), acquatici, cingolati);
- robot "*killer*" in grado di selezionare gli obiettivi da colpire, scegliendo, al contempo, come e quando attaccarli senza alcun intervento umano. Sperimentazioni sono in atto da parte di vari Paesi, ma l'unica applicazione pratica è rappresentata da un robot-sentinella che vigila sulla zona demilitarizzata tra le due Coree, dotato di videocamere a infrarossi, mitragliatrice e lanciagranate, in grado di individuare e colpire bersagli in movimento in un raggio di 3,2 km (per il momento ancora comandato a distanza, ma sono in corso ricerche per la completa automatizzazione);
- esoscheletri integrati indossati da un operatore umano (progetti Talos negli Stati Uniti e Ratnik in Russia), primo stadio per la creazione di futuri *cyborg*;
- droni – tecnicamente UAV, acronimo di *Unmanned Aerial Vehicle(s)* – equipaggiati anche di sistemi d'arma (es. droni Predator degli USA nel conflitto con l'ISIS) e organizzati in sciami (*swarm technology*), con la capacità di imitare artificialmente capacità collaborative (es. sistema LOCUST negli USA), che potranno essere abbinati a sistemi di controllo avanzati grazie allo sviluppo di interfacce neurali.

5.1.4. La risposta penalistica: problemi, limiti e prospettive.

5.1.4.1. L'avvento degli strumenti di A.I. per compiere fatti che astrattamente costituiscono reati solleva una serie di quesiti che mettono in forte evidenza i limiti dell'attuale ordinamento e quelli della risposta penalistica in senso tradizionale.

La questione più delicata – sul piano filosofico ed etico, prima ancora che giuridico – è senz'altro quella concernente la possibilità di concepire le entità intelligenti

come autori di reato. I sistemi di Intelligenza Artificiale di ultima generazione sono infatti dotati di un grado di autonomia dall'uomo tale da mettere in crisi il modello tradizionale della responsabilità indiretta di quest'ultimo per i fatti di reato verificatisi a causa del comportamento dell'entità di Intelligenza Artificiale.

Ciò non toglie, tuttavia, che le esigenze di repressione penalistica siano ancora attuali.

In questo senso, a fronte del crescente aumento di fenomeni subdoli e gravemente lesivi dei diritti individuali, anche costituzionalmente garantiti (la libertà di espressione e di coscienza, il diritto ad un voto libero e consapevole, la tutela da condotte discriminatorie) si avverte più forte la necessità di una regolamentazione giuridica e di un intervento normativo che sanzioni – anche penalmente – condotte che ledono o pongono in pericolo tali diritti, per finalità inibitorie e deterrenti, non essendo sufficiente affidarsi alle raccomandazioni o indicazioni del *soft law*.

La forma della riposta penale, antropocentrica e legata al concetto di "autore di condotte costituenti reato" e all'elemento psicologico del reato (in termini di dolo o colpa) appare tuttavia limitativa rispetto ad azioni condotte da macchine e da algoritmi di intelligenza artificiale in assenza di qualunque intervento umano (che non sia quello della creazione degli algoritmi e dell'avvio dei processi).

Né è pensabile di introdurre nuove e larvate forme di responsabilità oggettiva a carico delle persone fisiche.

5.1.4.2. A ben vedere, la difficoltà maggiore è costituita dai meccanismi di azione "diffusa" dell'A.I.:

- quasi mai è identificabile come autore di un reato un singolo soggetto, poiché le azioni sono condotte con metodo diffuso e attraverso macchine, programmi e *bot net* che nascondono la propria "identità" (reale o virtuale);
- l'azione di un'I.A. è "latente" e sfrutta le capacità di condizionamento di singoli utenti fisici che ne "amplificano" l'effetto attraverso propri comportamenti non sempre consapevoli (si pensi alle *deep fakes* che vengono condivise migliaia e milioni di volte su diverse piattaforme)
- per la stessa ragione è difficile individuare l'origine dell'azione dell'A.I., che quasi sempre travalica i confini nazionali (e delle giurisdizioni) e si muove nel *cyberspace* in modo globale.

Ancora, si è rilevato che:

- i reati commessi mediate l'utilizzo di sistemi informatici presentano elementi oggettivi di un'azione "riconoscibile" e individuabile mentre nel cyberspazio la nozione di azione "sfuma" e diventa difficilmente riconoscibile, e tende a sovrapporsi con l'evento che ne è il prodotto.
- Nel caso di I.A., in ragione delle logiche di apprendimento "autonomo" della macchina (*machine learning*) sembrano addirittura spezzare questo fragile nesso tra azione ed evento per cui il secondo è effettivamente il prodotto o l'effetto della prima, per spostare invece l'attenzione sulle regole "logiche" (e dunque loro effetti) con cui la macchina è programmata e sugli effetti. Su questo punto l'art 115 c.p. e il principio del

nemo cogitationis poenam patitur sembrano scontrarsi con l'idea di una punibilità del soggetto che ha concepito un programma le logiche e/o gli algoritmi con cui la macchina opererà successivamente

- Come ha scritto il dott. Fabio Di Vizio, l'azione dell'individuo nella maggior parte dei casi non è quella descritta dal "fatto" del reato, ma sarà l'esecuzione automatica da parte dei sistemi informatici a rilevare per la tipicità della norma incriminatrice

5.1.4.3. Esistono alcuni istituti penali o para-penali che potrebbero offrire risposte almeno parziali ad alcuni di questi problemi.

Su un primo versante, si è ipotizzato di utilizzare lo schema della posizione di garanzia (40, co. 2, c.p.) per individuare soggetti o enti qualificati chiamati a prevenire o impedire determinati eventi causati dall'I.A.

Il ricorso a reati omissivi impropri può essere uno schema di costruzione della fattispecie penale, responsabilizzare chi gestisce determinate piattaforme o programmi che utilizzano A.I. oppure su cui si manifestano i suoi effetti (es i social media); altro strumento utile potrebbe essere la configurazione di delitti c.d. di attentato, attraverso i quali si realizza un'anticipazione della tutela dei beni protetti, specie quando questi hanno natura super-individuale e diffusa.

Un'ulteriore linea di intervento è offerta dal superamento della prospettiva strettamente penalistica, mediante un rafforzamento della disciplina in materia di responsabilità degli enti (d.lgs. 231/2001), in particolare grazie alla previsione di misure interdittive più incisive.

5.1.4.4. Tuttavia, le prospettive appena esaminate pongono alcuni problemi derivanti dal possibile attrito con i principi generali del diritto penale e con i diritti fondamentali della persona.

In primo luogo, per quanto riguarda la previsione di obblighi di controllo in capo ai gestori di piattaforme (siano persone fisiche o enti), occorre valutare attentamente la concreta esigibilità delle misure preventive, non potendosi ammettere una responsabilità da posizione.

Ancora, l'attribuzione a determinati soggetti (piattaforme social o autorità governative) di poteri e obblighi di repressione e persino di prevenzione rispetto al verificarsi di determinati illeciti – anche tramite interruzione delle condotte che condurrebbero al verificarsi dell'evento atteso – sollevano indubbiamente un problema di bilanciamento degli interessi e di tutela di diritti costituzionalmente garantiti, in particolare con la libertà di manifestazione del pensiero, anche negli spazi virtuali

Il tema diventa delicato soprattutto in ambito di influenza sul mercato politico, e in generale quando si discorre di utilizzo di piattaforme di social media, che vedono ormai il web come strumento di espressione potenziata del proprio pensiero e forma di estrinsecazione pubblica della propria personalità.

La possibilità concessa dall'ordinamento (a un singolo soggetto, agli organi di una piattaforma ovvero ad un'autorità amministrativa) di intervenire bloccando la possibilità di condividere o pubblicare un determinato contenuto, "oscurandolo" e rimuovendolo all'accesso della platea di destinatari a cui era diretto, può costituire – specialmente si si tratta di materiale ideologicamente orientato – una forma di censura del pensiero, e divenire essa stessa forma di oppressione di minoranze e di repressione del dissenso politico.

D'altra parte, possono venire in rilievo anche altri diritti fondamentali: esistono varie forme di arti visive che si manifestano attraverso deliberati prodotti di A.I. e mediante *deep fake*.

Tutti questi casi sollevano due ordini di problemi: *a)* chi decide che un intervento di A.I. rappresenta una *fake news* o un *deep fake*? *b)* a quali condizioni e limiti è possibile un intervento repressivo o interdittivo?

Come visto, proprio nel caso del Gabon il ventilato sospetto che sedicenti "gruppi di potere" nascondessero la verità o volessero alterarla ha dato la stura a interventi di natura repressiva tipica di regimi totalitari e comunque non democratici.

Analogamente, proprio nel caso delle recenti elezioni U.S.A., gli interventi di rimozione, da parte delle piattaforme social più note, dei profili e dei contenuti ritenuti costituire delle *fake news* hanno provocato la reazione di numerosi cittadini che avevano pubblicato e commentato tali contenuti e che hanno lamentato la violazione della propria libertà di manifestazione del pensiero.

5.1.4.5. La domanda di frontiera resta però sempre: *machina delinquere potest*?

È stato osservato in dottrina che gli originari sistemi di A.I., che necessitavano dell'intervento remoto umano e che offrivano risultati tendenzialmente prevedibili (rappresentando dunque un mero strumento dell'azione umana) non ponevano seri problemi di crisi dello schema penale, potendosi individuare e punire con gli schemi tradizionali l'essere umano che è possessore e gestisce un mezzo materiale per compiere la propria condotta.

Tale schema appare probabilmente ancora utilizzabile nei casi di droni e sottomarini automatizzati programmati e utilizzati per compiere attentati, azioni lesive o per il narcotraffico.

Tuttavia, grazie ai meccanismi di apprendimento automatico (*machine learning*), un algoritmo è capace di imparare dall'esperienza e di modificare di conseguenza il proprio comportamento, adattandolo agli stimoli nel frattempo ricevuti. In molti casi, peraltro, mediante il ricorso alle tecnologie di *cloud computing* e alla raccolta di *big data*, un algoritmo, scambiandosi informazioni con altre, anche operanti in ambienti diversi, può incrementare esponenzialmente il proprio apprendimento.

È evidente, allora, che il comportamento di tali sistemi di Intelligenza Artificiale non è interamente predeterminato, e potrebbe persino essere *non prevedibile*.

In tali casi appare arduo individuare un autore umano e muovere un rimprovero alla persona fisica per il fatto di reato che si è verificato a causa di azioni impreviste della macchina dovute ad apprendimenti secondari; peraltro, secondo una interpretazione

conforme al principio costituzionale di personalità della responsabilità penale, l'autore non potrà essere chiamato a rispondere penalmente neppure in termini di *aberratio* (che richiede pur sempre la prevedibilità in concreto dell'offesa).

In effetti, è stato osservato che il funzionamento degli agenti intelligenti di ultima generazione basato sulle tecniche di *deep learning* dà luogo a quelli che sono definiti *black box algorithms*. In queste tecnologie il processo che dagli *input* conduce agli *output* rimane avvolto da un inevitabile grado di opacità nei passaggi logici seguiti, per cui non si riesce a comprendere come l'algoritmo abbia raggiunto il risultato finale, il quale rimane al di fuori delle capacità previsionali degli stessi programmatori[127].

Inoltre, già sul piano oggettivo, le logiche di apprendimento "autonomo" della macchina sembrano addirittura spezzare il nesso tra azione umana ed evento, per spostare invece l'attenzione sulle regole "logiche" con cui la macchina è programmata e sugli effetti. Su questo punto l'art 115 c.p. e il principio del *nemo cogitationis poenam patitur* sembrano scontrarsi con l'idea di una punibilità del soggetto che ha concepito e disegnato gli algoritmi con cui la macchina opererà successivamente.

5.1.4.6. Sul tema dei profili di responsabilità delle macchine, in **dottrina** si profilano due orientamenti.

(i) Secondo alcuni (Hallevy) non ci sono più ostacoli logici e giuridici che possano impedire di concepire le macchine di A.I. come soggetti attivi del reato, superando l'assioma del *machina delinquere* (*et puniri*) *non potest*.

Tali studiosi incentrano il ragionamento sull'elemento oggettivo del reato (condotta/evento) apprezzato in termini puramente materialistici (com'è negli ordinamenti di *common law*) compatibili direttamente con l'operatività del sistema di intelligenza artificiale, sia che si tratti di una condotta attiva (integrata da un movimento fisicamente apprezzabile della macchina: ad esempio, il movimento di un braccio robotico) sia che si tratti di un'omissione (integrata dall'inerzia della macchina).

Non muterebbe quindi il meccanismo logico di attribuzione della responsabilità; ciò che cambierebbe è solo la tipologia di sanzione, che dovrebbe essere adeguata ad incidere su una macchina (es. distruzione del corpo fisico, disattivazione e isolamento, o ancora riprogrammazione forzata, etc.)

Peraltro, con una ricostruzione meritevole di interesse, Hallevy si è spinto a ipotizzare tre paradigmi di responsabilità, tutti fondati sul presupposto necessario del riconoscimento della personalità giuridica alle entità intelligenti.

Il primo, definito *perpetration through another*, rappresenta l'aggiornamento di quello, tradizionale, di responsabilità indiretta dell'uomo: in base ad esso, i sistemi di I.A. sono strumentalizzati per la commissione del reato da una persona umana, che potrà

---

[127] S. DONCIEUX – J. MOURET, *Beyond black-box optimization: a review of selective pressures for evolutionary robotics*, in *Evolutionary Intelligence*, 7, 2014, 71 ss.; S. BECK, *Google cars, software agents, autonomous weapons systems – New challenges for criminal law?*, in E. Hilgendorf – U. Seidel (eds.), *Robotics, Autonomics, and the Law*, Baden-Baden, 2017, 227 ss.

individuarsi nel programmatore del *software* o nell'utente finale, e che ne risponderà in via esclusiva;

Il secondo (*natural probable consequence*) e il terzo (*direct liability*) paradigma prevedono, invece, la possibilità di individuare una responsabilità dell'entità intelligente, in via cumulativa o autonoma rispetto alla responsabilità di programmatore e/o dell'utente.

(ii) La tesi prevalente tra gli studiosi invece si orientano in senso negativo evidenziando l'inadeguatezza del sistema penale, i cui comandi (e sanzioni) sono concepiti come diretti a "uomini", in grado di provare timore e senso di deterrenza rispetto alla violazione, e a cui si rivolge la pena in senso "rieducativo".

Si obietta infatti che al riconoscimento dei sistemi di intelligenza artificiale come soggetti attivi del reato osta il principio di colpevolezza che informa di sé gli ordinamenti penali moderni.

Inoltre, i sistemi di intelligenza artificiale non sono capaci di provare timore e sono quindi immuni dall'effetto dissuasivo della minaccia della pena (prevenzione generale) e, tantomeno sono in grado di cogliere l'effetto pedagogico connesso alla comminatoria legislativa della sanzione e quello di accreditamento sociale dei valori tutelati.

Inutile sarebbe anche la funzione di prevenzione speciale – intesa, alla stregua del principio costituzionale della finalità rieducativa della pena, come risocializzazione – in quanto inapplicabile ai sistemi robotici e di intelligenza artificiale.

La sanzione potrebbe dunque funzionare solo come mera neutralizzazione o riprogrammazione forzata, secondo concetti incompatibili con le categorie del diritto penale attuale.

A livello pratico, anche tale dottrina riconosce che le uniche possibili soluzioni alternative al sistema penale sono due: o si vieta radicalmente la realizzazione di tali sistemi, in base al principio di precauzione (es. droni autonomi armati), con la conseguente rinuncia ai benefici sociali apportati dagli stessi; oppure si individua un'area di rischio consentito, attraverso complessi bilanciamenti tra l'utilità collettiva e i rischi imponderabili dei vari sistemi e tali azioni non verranno punite (es. auto a guida autonoma).

5.1.4.7. I recenti interventi normativi dell'Unione europea si pongono il problema dei rischi dell'utilizzo di sistemi che impiegano I.A. in diversi campi, anche per il possibile impatto sui diritti fondamentali delle persone, ma non affrontano il tema della responsabilità, anche sotto il profilo penale, se non in senso tradizionale della necessità di una "*governance*" umana dell'A.I., di soggetti fisici che la controllano e governano e "devono" intervenire per "correggerla". Restano però aperte una serie di questioni: cosa accade ai danni o alle aggressioni già prodotte? chi può giudicare? a quali condizioni? Se si traducono in condotte costituenti reato a quali condizioni è possibile punirle e in quale ordinamento giudiziario?

Tali quesiti non trovano risposta neppure nei documenti più recenti:

- La **Risoluzione del Parlamento europeo del 20 gennaio 2021**[128] con le *linee guida per l'uso dell'Intelligenza artificiale in campo civile e militare*, fissa la necessità di disporre di un quadro giuridico europeo comune, con definizioni armonizzate *e* principi etici comuni, ma ribadisce che L'I.A. utilizzata in un contesto militare e civile deve essere soggetta ad un significativo controllo umano, in modo tale che in qualsiasi momento un umano abbia i mezzi per correggerla, bloccarla o disattivarla in caso di comportamento imprevisto. Ma ciò significa che è l'umano che ne risponde? Cosa accade se il fatto è imputabile a uno Stato o un suo organo fondamentale? Ma soprattutto: come è possibile che ne risponda se non è un membro UE e se non ha adottato i "principi etici e le definizioni armonizzate"?
- La **Proposta di Regolamento** del Parlamento Europeo e del Consiglio del 21 aprile 2021[129] che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione - 2021/0106 (COD) classifica i prodotti che utilizzano software di A.I. in base al rischio di impatto negativo su diritti fondamentali quali la dignità umana, la libertà, l'uguaglianza, la democrazia, il diritto alla non discriminazione, la protezione dei dati e, in particolare, la salute e la sicurezza. La proposta si pone in una prospettiva di divieto di utilizzo di alcuni sistemi di I.A. e di rigoroso controllo, ma non prevede sanzioni né si occupa degli aspetti penali e giudiziari delle violazioni.
- La **Risoluzione del Parlamento europeo del 6 ottobre 2021**[130] sull'**intelligenza artificiale nel diritto penale** e il suo **utilizzo da parte delle autorità di polizia e giudiziarie** in ambito penale (2020/2016(INI)) è finalizzata ad evidenziare i rischi che possano derivare dall'utilizzo di strumenti di I.A., specialmente nel contesto dell'*enforcement* penale e della sorveglianza pubblica, ponendosi in una prospettiva che punta a limitare l'uso di queste tecnologie.

5.1.4.8. Sorgono inoltre notevoli problematiche in relazione all'applicazione spaziale della legge penale e al *tempus commissi delicti*.

Il cyberspazio non ubbidisce alla logica territoriale dei confini nazionali (per sua natura è infatti a-territoriale), a differenza degli ordinamenti statali che richiedono uno «spazio sul quale esercitare la propria sovranità esclusiva».

Infatti, la rete permette all'individuo, di essere presente e operare anche simultaneamente in più "luoghi informatici". Ciò comporta la de-temporalizzazione delle azioni, ossia programmare e automatizzare complesse operazioni senza il necessario e simultaneo "contatto fisico" tra uomo e sistema informatico. Si pensi, in particolare, alla realizzazione di *criminal smart contracts* dove è possibile pianificare a monte il software, la cui esecuzione causerà l'evento rilevante per la norma incriminatrice solo successivamente e al verificarsi di determinate condizioni previamente stabilite ed automaticamente eseguite. Tali sistemi "distanziano", creando

[128] Cfr. https://www.europarl.europa.eu/doceo/document/TA-9-2021-0009_IT.html.
[129] Cfr. https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52021PC0206&from=IT.
[130] Cfr. https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_IT.html.

tra loro un gap spaziale e temporale, l'agente fisico e la macchina che sarà autore-materiale di un crimine.

Analogamente, nei fenomeni di *deep fake*, delle azioni ai danni di sistemi economici e politici degli Stati l'azione di destabilizzazione può essere subdola, operare in simultanea da più contesti spaziali e cronologicamente ripetuta nel tempo sfruttando più "co-autori inconsapevoli" o in buona fede (si pensi ai movimenti no-vax che vengono mossi e manipolati per anni sulla base di *deep fake* introdotte e manipolate in rete da piccoli gruppi di individui; o ancora, agli estremisti di destra che alimentano il proprio odio razziale o antisemita in base a finti documenti che circolano in rete e veicolati da gruppi che si dicono in possesso della "verità" e di un "sistema" di controinformazione).

Come noto, è fondamentale determinare quando un reato può ritenersi commesso nel territorio italiano.

Diverse sono le soluzioni prospettabili quando vengono in rilievo reati commessi mediante I.A.

Una prima tesi potrebbe essere quella di considerare il crimine commesso nel luogo in cui gli attori hanno avviato l'*azione* (di manipolazione o di creazione e inserimento in rete delle notizie false).

In caso di azione simultanea in più contesti spaziali si potrebbe pensare ad un meccanismo simile a quello degli artt. 12-16 c.p.p.; tuttavia, risulta fonte di difficoltà applicative l'ineliminabile incertezza sul "dove" l'azione è stata "compiuta", anche in parte.

Un ostacolo concreto alla verificazione del luogo geografico dell'individuo che compie azioni lesive è costituito dall'utilizzo di VPN (*virtual private network*) e di browser con crittografia stratificata. Dal punto di vista informatico, anche se fisicamente il soggetto agente opera da un computer situato in Italia, risulterà come connesso a server ubicati in altri paesi, creando così difficoltà anche dal punto di vista probatorio.

Un criterio diverso potrebbe essere quello che fa leva sull'*evento* finale (ossia sul "prodotto" o sugli effetti negativi delle azioni di I.A.), che se verificatosi in territorio nazionale potrebbe radicare la giurisdizione.

Anche questo criterio non garantisce soluzioni semplici e immediate, poiché la sua applicazione potrebbe scontrarsi con la volontà di altri Stati di affermare la propria giurisdizione, con la mancanza di regole condivise a livello internazionale in tema di individuazione e acquisizione delle prove e con le difficoltà legate allo svolgimento di indagini su "entità" e soggetti responsabili dell'attacco anche in territori soggetti a sovranità e giurisdizione "altrui".

Peraltro, in materia di ordine pubblico e di terrorismo in particolare, la casistica ci pone di fronte a "eventi diffusi" di cui non è semplice la localizzazione territoriale[131].

[131] Sulla struttura "a rete" delle associazioni terroristiche attuali, specie di matrice jihadista (es. ISIS), capaci di operare contemporaneamente in più Stati attraverso cellule che comunicano reciprocamente a distanza e in modo sporadico, cfr. Cass., sez. V, 13 luglio 2017 (dep. 3 novembre 2017), n. 50189; Cass., Sez. VI, sent. 19 dicembre 2017 (dep. 29 marzo 2018), n. 14503.

5.2. I.A. e Law Enforcement.

I sistemi di I.A. possono essere impiegati anche per **finalità "benigne"**:
- in attività di **contrasto e disvelamento dei reati** commessi mediante intelligenza artificiale;
- nelle attività rivolte alla **prevenzione dei reati**, dedicando particolare attenzione allo specifico ambito denominato **"polizia predittiva"** (*"predictive policing"*)

5.2.1. Attività di indagine tramite I.A.: alcuni esempi concreti tratti dall'esperienza italiana.

Le forze dell'ordine hanno ultimamente incrementato la propria capacità operativa in materia di prevenzione e repressione di reati anche grazie all'adozione di strumenti investigativi basati sull'intelligenza artificiale.

In Italia, nell'ambito delle attività di pubblica sicurezza, sono oggi correntemente in dotazione alle forze dell'ordine sistemi di analisi dati, riconoscimento e allarme interamente automatizzati e utilizzabili tramite smartphone o tablet (O.D.I.N.O. in uso all'Arma dei Carabinieri e Mercurio adottato dalla Polizia di Stato). Un *software* apposito (S.A.R.I.) svolge funzioni di riconoscimento facciale consentendo di identificare un soggetto a partire da un fotogramma, confrontando quest'ultimo con banche dati contenti dati biometrici e fotografie o con le immagini delle telecamere di sorveglianza di una determinata zona.

È stato altresì sviluppato un primo software di polizia predittiva (*X-Law*) che, attraverso l'approccio del *machine learning*, attinge ai dati provenienti dall'archivio denunce e li compara con quelli sulle caratteristiche socioeconomiche e demografiche locali e sugli eventi in programma, per fornire precisi avvisi geolocalizzati circa l'alta probabilità di verificazione di un crimine in una data area (specie per i reati predatori urbani).

Sono poi in fase di sviluppo o sperimentazioni sistemi ulteriori.

Tra questi sono sicuramente di rilievo i sistemi c.d. Virtual HUMINT, sviluppo tecnologico della tradizionale attività di *human intelligence* (basata sull'interazione interpersonale svolta da persone fisiche) che offre maggiori garanzie di sicurezza, anonimato e rapidità di accesso. La tecnologia in questione consente di creare avatar per monitorare o avvicinare profili-bersaglio mantenendo la copertura grazie ad algoritmi progettati per imitare il comportamento umano (ed evitare di essere così identificati come robot) e per evitare la tracciabilità dell'operatore e della sua organizzazione di appartenenza.

5.2.2. Criticità teoriche e pratiche.

L'utilizzo massiccio di A.I. per scopi di *law enforcement* costituisce già una realtà in diversi Stati (così soprattutto negli USA), dove sono state già poste in evidenza varie problematiche applicative ed etiche[132].

- In primo luogo, sono sorti interrogativi sui margini di autonomia di tali applicazioni che utilizzano sistemi di intelligenza artificiale rispetto al controllo umano: il controllo dell'uomo si deve limitare alla scelta degli obiettivi, al monitoraggio, o deve essere un controllo più intenso, esercitato anche a costo di compromettere le prestazioni?
- Un secondo problema è quello della privacy rispetto alla gran mole di dati che queste applicazioni (fornite, ad esempio, di sensori e telecamere avanzate) possono acquisire in relazione alla vita, anche privata, dei cittadini, e che potrebbero essere manipolati abusivamente, sottratti, deformati, con grave pregiudizio per le persone cui essi si riferiscono.
- Vi sono indubbie preoccupazioni in ordine al tasso di fallibilità di queste applicazioni e quindi in ordine all'individuazione del reale responsabile (uomo o macchina?) di eventuali uccisioni o lesioni commesse per errore, specialmente in caso di dispositivi robotizzati armati, che sono inevitabilmente privi delle doti tipicamente umane come la pietà, l'intuito, la capacità di improvvisazione, il c.d. senso comune, che possono bloccare ed evitare errori.
- La predizione si basa fondamentalmente su una rielaborazione attuariale di diversi tipi di dati: tra i dati inseriti talora compaiono anche informazioni relative all'origine etnica, al livello di scolarizzazione, alle condizioni economiche, alle caratteristiche somatiche riconducibili a soggetti appartenenti a determinate categorie criminologiche (ad es., potenziali terroristi), etc., che potrebbero portare ad effetti finali di natura discriminatoria o di rafforzamento di pregiudizi culturale/sociale.
- Di contro, la deliberata omissione di alcuni dati, specie in rapporto agli altri, può minare l'effettiva validità predittiva (*accuracy*) e all'imparzialità (*fairness*) di questi algoritmi, i quali potrebbero produrre risultati poco affidabili o comunque discriminatori.
- Vi sono poi problemi di trasparenza/opacità di non poco momento: si pensi solo al fatto che gli imputati, ma anche gli stessi giudici, in molti casi (ad esempio, nel caso di COMPAS, software utilizzato negli Stati Uniti per prevedere la probabilità di recidiva di un imputato) non hanno dettagli in ordine al funzionamento interno degli *algoritmi*, giacché tali informazioni sono coperte da segreto industriale; risultato fornito dagli algoritmi predittivi è necessariamente influenzato dalla *qualità* dei dati che vengono posti come *input*;

[132] Cfr. F. BASILE, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Diritto penale contemporaneo*, 29 settembre 2019 (https://archiviodpc.dirittopenaleuomo.org/d/6821-intelligenza-artificiale-e-diritto-penale-quattro-possibili-percorsi-di-indagine).

5.2.3. Principi per una possibile regolamentazione.

I rischi e le esigenze di tutela passate in rassegna impongono – in vista di una futura disciplina normativa della materia – regole e procedure che assicurino:

- la qualità del dato, l'indipendenza della fonte da cui provengono i dati, l'indipendenza del soggetto che raccoglie i dati;
- l'accessibilità di tutti dei dati posti come *input* dell'algoritmo e la trasparenza delle parti essenziali dello stesso e dei suoi meccanismi decisionali;
- la prevenzione di esiti discriminatori del processo decisionale per ragioni legate a dati personali sensibili, tra cui la razza e l'estrazione sociale, l'orientamento religioso o politico o sessuale;
- la verificabilità della struttura dell'algoritmo.

È ormai noto ma merita di essere ribadito che la struttura di un algoritmo non è mai *neutra* poiché il programmatore fa delle scelte che, necessariamente, influenzano il *risultato* dell'operazione computazionale; il programmatore può fare degli errori di progettazione; un algoritmo la cui struttura sia protetta da diritti di proprietà intellettuale e non *open source* è sottratto alla possibilità di controllo, verifica e confutazione da parte della parte processuale.

Si segnala che in Europa, allo stato, gli algoritmi predittivi della pericolosità criminale (e, più in generale, gli *automated decision systems*), non hanno avuto accesso nelle nostre aule penali, anche perché, a precludere loro l'accesso, si erge l'art. 15 della direttiva 95/46/CE, confluito nell'art. 22 del nuovo Regolamento europeo in materia di protezione dei dati personali, entrato in vigore il 25 maggio 2018. Tale articolo stabilisce, infatti, che ogni persona ha il diritto di non essere sottoposta ad una decisione che produca effetti giuridici o abbia effetti significativi nei suoi confronti fondata *esclusivamente su un trattamento automatizzato di dati* destinati a valutare taluni aspetti della sua personalità.

Sempre in ambito Europeo, occorre altresì ricordare che la Risoluzione del Parlamento europeo sulla robotica del 2017[133] pone l'accento proprio sul *principio della trasparenza*, sottolineando la necessità che risulti sempre possibile spiegare la logica alla base di ogni decisione, presa con l'ausilio dell'intelligenza artificiale, qualora tale decisione possa avere un impatto rilevante sulla vita di una o più persone.

6. Conclusioni e proposte.

All'esito della ricognizione svolta è stato possibile individuare alcune questioni meritevoli di approfondimento prioritario.

In particolare, a fronte di una fenomenologia criminale assai varia, ineludibile pare il problema della giurisdizione e – in parallelo – dell'elaborazione di regole di

[133] Cfr. https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX:52017IP0051.

diritto cogente che, innovando o superando le categorie tradizionali, possano tenere conto delle peculiarità del *cyberspace*.

Si sono viste le difficoltà di inquadrare con i consueti istituti penalistici fenomeni nuovi ed estremamente complessi, in cui l'autore fisico assume una posizione sempre più marginale nella realizzazione del fatto, mentre la sfida attuale – ancora solo in parte esplorata dalla dottrina – ruota intorno alla possibilità di ravvisare profili di responsabilità direttamente in capo alla macchina.

Sul versante della giurisdizione, il carattere transnazionale dei *cybercrimes* pone difficoltà che non possono tuttavia portare a rinunciare a essenziali esigenze di garanzia e di affermazione di diritti e doveri degli Stati, degli organismi intermedi e dei singoli.

Al contempo, la rapidità delle condotte realizzate mediante I.A. evidenzia le criticità in cui incorrono i classici strumenti della cooperazione internazionale.

Gli ultimi documenti – sia a livello NATO che UE – sembrano andare nella prospettiva della neutralizzazione con una risposta più o meno occulta ad azioni di A.I. aggressive, il che tuttavia genera il rischio di innescare conflitti tra gli Stati (anche per effetto delle inevitabili controversie circa l'identificabilità della provenienza soggettiva e territoriale dell'azione lesiva). È uno scenario che chiede cautela, perché solo in parte sono prevedibili i rischi di uno scenario in cui la sovranità dello Stato dovrà cedere ad "azioni preventive" di attori spesso occulti (servizi di intelligence e simili) o di organismi militari, con effetti simili a quelli di un conflitto bellico, anche per il possibile impatto sulle infrastrutture critiche di ciascuna nazione.

Alla luce di questi punti problematici, la proposta del Gruppo anche nell'ottica della prosecuzione della ricerca è quella di attribuire centralità al momento processuale: la necessità di reprimere e di prevenire da un lato, e di rispetto dei diritti fondamentali dall'altro, possono e devono trovare una convergenza all'interno del processo, quale istituto di garanzia, composizione e tutela di tutti gli interessi in gioco.

Oltre a tale considerazione generale, i prossimi passi dovrebbero consistere

1) nell'elaborazione di regole condivise funzionali alla tutela di beni giuridici universali, con revisione delle Convenzioni di Budapest e di Palermo;

2) nell'elaborazione di nuove regole e nella predisposizione di nuovi strumenti tecnologici in grado di garantire l'acquisizione degli elementi di prova e la loro utilizzabilità in sede processuale.

I.A. e reati "comuni"

di Mario Palazzi
Sostituto Procuratore Tribunale di Roma

SOMMARIO: 1. Premessa. – 1.1. Ricognizione delle principali tematiche di lavoro e primi approfondimenti. – 2. L'intelligenza artificiale "nelle cose". – 3. *Blockchain*, *smart contracts*, D.A.O. (*Decentralized Autonomus Organization*) quali nuovi strumenti per il riciclaggio. – 4. L'I.A. come vittima di reati. – 5. L'intelligenza artificiale ed il contrasto alla pedopornografia.

1. Premessa.

Il diritto penale, terreno non solo della funzione del punire, ma della difesa degli interessi metaindividuali nella cornice del pieno rispetto di regole di garanzia, è strettamente legato a concetti tradizionalmente ritenuti immutabili, che oggi invero appaiono irrimediabilmente in crisi.

La sovranità, quantomeno nella sua accezione tradizionale, non sembra più appartenere (solamente) allo Stato-nazione e i singoli elementi che la compongono sono appannaggio di agenzie sovranazionali o a grandi imprese multinazionali.

Nel *web* operano, approfittando di una sostanziale *deregulation*, strutture di ogni genere, a partire da quelle lecite, che pure tendono ad operare con logiche distorsive della libera concorrenza, fino a vere e proprie strutture criminali organizzate, attive nei settori più disparati.

Il sempre più ampio utilizzo dell'intelligenza artificiale (I.A.) in numerosi settori tecnologici impatta quotidianamente, più di quanto si abbia effettiva contezza, nelle relazioni sociali, economiche e giuridiche.

Si tratta di tecnologie che presentano indubbie potenzialità, contribuendo non solo ad incrementare l'efficienza dei servizi resi, ma ne rendono possibili alcuni fino ad ora solo immaginabili.

Al tempo stesso, però, questi strumenti implicano innegabili rischi e criticità, soprattutto quando li si voglia applicare negli ambiti che coinvolgono più immediatamente diritti e libertà individuali.

Quello dei rapporti tra intelligenza artificiale e diritto e giustizia penale è un profilo particolarmente complesso, a causa delle molteplici modalità nelle quali gli algoritmi possono venire in rilievo: come strumenti a vario titolo coinvolti nella commissione di reati, ovvero come strumenti di supporto all'attività del pubblico ministero o delle forze dell'ordine (cosiddetta polizia predittiva), ovvero ancora come strumento di supporto all'attività dell'organo giudicante (cosiddetta giustizia predittiva).

Si tratta, è evidente, di un settore dell'ordinamento nel quale la tenuta delle garanzie individuali e dei principi dello Stato di diritto va assicurata con maggior vigore.

Le stesse definizioni di intelligenza artificiale, variamente proposte, soffrono di estrema elasticità, tale da vanificare l'opera stessa di definizione.

In prima approssimazione, il ragionamento attraverso cui il sistema informatico elabora i dati ha un nome: algoritmo. Si tratta di una procedura ben definita volta alla trasformazione di dati di *input* in dati di *output*. Nei sistemi dotati di intelligenza artificiale, la macchina è dotata di un algoritmo – il c.d. *metalgoritmo* – capace di costruire da sé nuovi algoritmi e idoneo a definire un nuovo processo di trasformazione, a seconda del problema di volta in volta rappresentato.

La macchina non è capace di porre domande, ma sa costruire risposte, anche attraverso meccanismi ignoti al suo programmatore. È in questo contesto che va inquadrato il fenomeno del *machine learning*, tale per cui la macchina migliora le sue prestazioni grazie all'esperienza; questo dispiega i suoi effetti anche sulla prevedibilità della risposta, essendo plausibile che il sistema operi attraverso procedure non più controllabili dal suo ideatore e non sempre verificabili *ex post*: una macchina che non è capace di conoscere o approfondire il problema, ma è capace, attraverso un'attività puramente computazionale, di risolverlo.

1.1. Ricognizione delle principali tematiche di lavoro e primi approfondimenti.

A fronte della vastità delle questioni da affrontare – poiché potenzialmente l'uso dell'A.I. può interferire su un catalogo pressoché indeterminato di fattispecie penali – una disamina omnicomprensiva è di fatto impossibile.

Il gruppo di lavoro – che beneficia di una molteplicità di professionalità ed esperienze, provenienti dalla magistratura, dall'università, dalle forze dell'ordine, dalla Banca d'Italia e dai principali *stakeholder* del mondo dell'impresa – ha necessariamente optato per una prima selezione di contesti maggiormente investiti dall'ingresso prepotente dell'I.A., al fine di individuarne caratteristiche, criticità, possibili soluzioni *de iure condito* piuttosto che *condendo.*

2. L'intelligenza artificiale "nelle cose".

Il primo problema che il giurista penale deve affrontare attiene al modello di imputazione della responsabilità degli eventi che vedono il contributo causale dei sistemi di Intelligenza Artificiale di ultima generazione, che operano in base ad algoritmi aperti ad automodifiche strutturali, determinate dall'esperienza del sistema stesso.

A fronte di tali sistemi il cui agire non è interamente predeterminato – e perciò prevedibile – ascrivere una responsabilità penale è un'operazione complessa, che investe categorie generali quali la causalità e la colpa.

Da tempo, ormai, il paradigma di ascendenza civilistica della responsabilità per danno da prodotto è entrato a pieno titolo anche nel mondo del diritto penale. I più svariati prodotti di origine industriale, infatti, in caso di errori di progettazione, manifattura, confezionamento, distribuzione, o ancora per un loro errato uso, possono

essere causa di eventi dannosi per la salute e l'incolumità dei soggetti umani che vi interagiscano. In tal caso, l'errore nell'utilizzazione o nel processo produttivo – ove si pervenga alla conclusione che si tratti di una violazione cautelare che ha dato luogo a danni *ex ante* prevedibili – può essere inquadrato come una condotta colposa causalmente connessa ad un evento di danno, sussumibile entro il perimetro delle più classiche fattispecie colpose di risultato previste dal codice penale.

Ora, lo sviluppo delle tecnologie dell'I.A. prospetta, per i prossimi anni, uno scenario in cui prodotti tecnologici "intelligenti" si affacceranno sul mercato, pronti a diffondersi rapidamente nel tessuto sociale e produttivo – salvo i limiti rispetto a ciò imposti da eventuali divieti di legge – inducendo così i produttori a potenziare ulteriormente quei profili di "autonomia" che costituiscono il *quid pluris* di tali prodotti rispetto a quelli più tradizionali.

Simili tecnologie sono in parte già in fase avanzata di sperimentazione. L'esempio forse più significativo è quello delle auto a guida autonoma, che come noto ormai da anni circolano sotto forma di prototipi sulle strade statunitensi, avendo peraltro già causato – pur con centinaia di migliaia di chilometri percorsi in sicurezza – plurimi sinistri, con esito talvolta mortale. Più di recente, peraltro, simili sperimentazioni sono state avviate anche in Italia. Ma non mancano altri settori nei quali gli sviluppi tecnologici hanno già reso realtà dei prodotti robotici "intelligenti" dall'indiscutibile potenziale commerciale, come ad esempio in ambito medico e militare.

La potenzialità di sviluppo di tali sistemi, poi, è immensa: basti pensare alla casa, in cui dalla iniziale domotica cablata si assiste a soluzioni *wireless* caratterizzate da servizi in *cloud* e dall'uso crescente dell'Intelligenza Artificiale. Oppure ancora ai luoghi di lavoro, con ripercussioni nella materia della prevenzione infortuni.

Rispetto alla fisionomia tradizionale dei meccanismi imputativi dell'evento colposo causato da un difetto di produzione o da un cattivo uso di un prodotto, la natura "intelligente" dei nuovi prodotti comporta difficoltà peculiari nell'attribuire la responsabilità per un danno verificatosi. La capacità delle I.A. di apprendere e di modificare i propri i comportamenti, in modo anche del tutto imprevedibile rispetto alla sua originaria programmazione, offusca infatti la possibilità di imputare ad un attore umano dietro la macchina la responsabilità per un evento cagionato dal comportamento del soggetto artificiale stesso.

Occorre valutare le diverse ripercussioni che la natura "intelligente" del prodotto proietta sull'imputazione del fatto alle due figure umane di riferimento: l'utilizzatore e il programmatore/produttore.

La possibilità di imputare l'evento lesivo della macchina al suo *utilizzatore* umano non è sempre e immediatamente negata dal carattere "intelligente" di questa. Fintantoché, infatti, permane la possibilità materiale di intervento dell'utilizzatore umano nel correggere "in corsa" il comportamento del soggetto artificiale, assieme a un obbligo giuridico di controllo e di intervento gravante in capo al primo (esattamente, un obbligo di protezione dal pericolo derivante dalla fonte artificiale intelligente), una colpa potrà sempre sussistere nel comportamento *lato sensu* omissivo dell'utilizzatore umano stesso. Si pensi al conducente di un'auto a guida autonoma, comunque ancora dotata di comandi.

Il nodo politico-regolativo, dunque, è quello relativo al fatto se sia opportuno che l'ordinamento imponga un simile obbligo di sorveglianza, oppure no. Una risposta positiva a tale quesito rischia di vanificare la gran parte dei vantaggi connessi al carattere "intelligente" del prodotto in questione, connessi proprio alla sua capacità di "fare da solo". Si può, peraltro, dubitare dell'efficacia in termini preventivi di un intervento umano correttivo in contesti ad elevata complessità, o che necessitino una reazione pronta dopo ore di mera sorveglianza passiva.

Al momento, la tendenza prevalente sul piano regolativo è quella di un "precauzionismo" estremo, volto a prevedere, in quei casi dove ancora non viga il divieto di attività artificiale intelligente *tout court*, capillari obblighi di controllo in base a cui mantenere la presenza di una figura umana cui imputare eventuali eventi lesivi che abbiano a verificarsi. L'alternativa, infatti, è quella del vuoto di responsabilità: prospettiva nella quale si ricade, inevitabilmente, per tutte quelle tecnologie che escludano in radice la possibilità di un intervento correttivo umano (es., *robotaxi* privi di comandi).

Anche la possibilità di imputare possibili eventi dannosi al *produttore*, ove il prodotto sia un soggetto artificiale intelligente, diviene di estrema complessità. Salva la difficoltà di individuare singole responsabilità penali individuali in un contesto organizzativo plurisoggettivo composito, emerge con forza la difficoltà di imputare al programmatore umano un fatto cagionato dalla macchina con un comportamento del tutto imprevedibile, perché derivato da quell'apprendimento che è tipico delle intelligenze artificiali.

In definitiva, il problema politico-regolativo che emerge dall'intersezione delle tecnologie dell'I.A. con il settore della responsabilità per danno da prodotto, o – per dirla in termini più ampi – del reato colposo, è quello del c.d. *responsibility gap*. Tale "vuoto di responsabilità" consiste nel fatto che è complesso, se non del tutto impossibile, imputare alcuni degli eventi lesivi provocati dal comportamento dei "prodotti-I.A." ad uno o più soggetti umani, i soli che possano rispondere sul piano della responsabilità penale personale.

Tale nodo problematico, lungi dall'avere rilievo meramente settoriale, è gravido di importanti ripercussioni di ordine generale, giacché interessa le scelte regolatorie che i singoli Stati sono chiamati a compiere in merito alla portata e ai limiti che simili tecnologie riscontreranno nel mercato legale. Il timore di vuoti di tutela per i beni primari della vita, sicurezza e salute umana, infatti, può ben alimentare la permanenza di politiche precauzionistiche e attendiste, che rallentino percorsi regolativi comunque presumibilmente tutti direzionati, in un futuro di lungo periodo, verso scenari di ampia autorizzazione.

3. *Blockchain, smart contracts, D.A.O. (Decentralized Autonomus Organization)* quali nuovi strumenti per il riciclaggio.

L'uso delle nuove tecnologie nel sistema finanziario a fini di riciclaggio e di finanziamento del terrorismo rappresenta indubbiamente l'aspetto più complesso e

preoccupante del rapporto tra I.A. e diritto penale, tanto da costituire oggetto prioritario di studio in seno al gruppo di lavoro.

È di comune esperienza l'esponenziale utilizzo di strumenti di trasferimento delle risorse attraverso la c.d. "polverizzazione dei contanti via *internet*" che, consentendo l'effettuazione di transazioni in un contesto a-territoriale, in modo affidabile e pseudo- anonimo, costituisce un metodo eccellente per mimetizzare la provenienza delittuosa delle risorse. La *blockchain*, in particolare, elimina un elemento fondamentale negli scambi commerciali degli ultimi secoli: il terzo garante.

Mediante il libro mastro decentrato, la *blockchain* sposta la funzione di garanzia dal singolo alla rete, permettendo ai partecipanti di scambiarsi dati in modo sicuro e senza doversi affidare a terzi.

Lo strumento normativo del regolatore nazionale ed internazionale per la prevenzione del riciclaggio e del finanziamento del terrorismo è quindi entrato in crisi; la responsabilizzazione di tutti quei soggetti i quali – data la loro funzione di intermediari – si pongono quali collettori di informazioni e che svolgono, in questo sistema, una funzione di allarme decentrato per le autorità investigative rischia, di fatto, di divenire una regola senza possibilità di applicazione.

Le criptovalute, operando su un sistema di scambio da pari a pari, eludono tutti quei soggetti che formano la struttura di allarme diffuso predisposto dal sistema AML/CFT.

L'ingresso massivo dell'intelligenza artificiale nella tecnologia *blockchain* rischia di rendere di fatto impossibile la ricostruzione *ex post* del "*paper trail*", a fronte di trasferimenti disintermediati, rapidissimi e occulti, tra soggetti allocati in giurisdizioni diverse.

Il tema degli *smart contract*, su cui pure si interroga la dottrina civilistica, appare una manifestazione di grande insidiosità: questi agenti-*software*, al verificarsi di certe condizioni, predeterminate dal programmatore e "attivate" dalle parti, daranno esecuzione al contratto, eseguendo in modo automatico la prestazione in esso dedotta.

Il tema è oggetto approfondito da altro gruppo di lavoro, proprio per le problematiche derivanti dall'utilizzo degli algoritmi di *trading* sui mercati finanziari e le relative implicazioni su piano della responsabilità penale per *market abuse.*

Le parti possono concordare sul contenuto di un contratto già registrato in *blockchain* ad opera di un terzo (*smart contract* improprio o di terza parte), ovvero concludere da sé un accordo in linguaggio computazionale (*smart contract* proprio).

Si pensi – quanto al primo caso – alla pubblicizzazione di un contratto *smart* che, al verificarsi di determinate condizioni, compia attività di *mixing*, movimentando valute virtuali su più conti intermedi, per poi permettere di recuperare le somme su un conto di destinazione, con la conseguenza – indubbiamente caratterizzata da causa illecita – di disperdere la tracciabilità dei flussi di transazioni iscritti sul registro pubblico, e con ciò riciclare proventi di origine delittuosa.

In questo particolare settore, il "mercato" rende disponibile le c.d. DAO (*Decentralized Autonomous Organization*), organizzazioni che operano seguendo esclusivamente regole imposte dal codice secondo il quale sono state programmate. Tali

organizzazioni operano in modo totalmente indipendente dai loro creatori e non possono essere influenzate in nessun modo dall'esterno.

Diviene allora centrale – ancor più dell'ascrivibilità di una condotta illecita al programmatore – il suo utilizzo. A livello legislativo, potrà eventualmente essere anticipata la soglia della rilevanza penale del fatto.

Altro insuperabile problema – con l'assetto normativo vigente – attiene alla a-territorialità e alla transnazionalità del sistema: questi strumenti si sostanziano in null'altro che annotazioni contabili su un registro, sul quale è indicato chi ha diritto a trasferire e quali somme. In tale contesto, l'utente – più che essere proprietario di determinate criptovalute – ha una pretesa rispetto al registro di poter ritrasferire un certo numero di *coins ad nutum*. Tale registro è per sua natura decentralizzato; ogni nodo della rete *blockchain* possiede una copia di tale registro e partecipa al processo di formazione del consenso per l'aggiunta dei successivi blocchi. Le criptovalute esistono contemporaneamente in ogni nodo che compone la *blockchain* di riferimento, il che vuol dire in più di un continente contemporaneamente.

La logica "tradizionale" di ampliamento dei destinatari degli obblighi di registrazione e *compliance* AML/CFT a tutti gli operatori che, a qualsiasi titolo, operino professionalmente nel mercato delle cripto-valute appare quindi una risposta ontologicamente insufficiente.

È indubbia la necessità di ripensare le direttrici del sistema regolatorio, così come il corpo normativo di repressione; in tale contesto, però, l'intelligenza artificiale rappresenta ad un tempo fattore di rischio e imprescindibile risorsa.

Ci si chiede se non si debba optare per un controllo sul registro mediante A.I. *based web crawlers*, i quali possano identificare *pattern* di transazioni sospette. A seguito di tale identificazione, le criptovalute associate a quella transazione potrebbero essere bloccate – mediante un sistema di *blacklisting* – richiedendo al possessore di identificarsi e giustificare la transazione stessa; tale blocco potrebbe essere operato tramite una presunzione di abusività del *pattern*, sulla falsariga di quanto accade in tema di accertamenti tributari.

Ovviamente, la creazione di tali *software* pongono rilevanti questioni in termini di valore probatorio delle segnalazioni effettuate, nonché il tema centrale del superamento dei limiti tradizionali utilizzati per la delimitazione delle giurisdizioni, a fronte di un fenomeno che si caratterizza per natura decentralizzata e pertanto essenzialmente a-territoriale delle reti.

Questi modelli di controllo impongono dunque una riflessione sovranazionale, con l'obiettivo di raggiungere nuove forme di cooperazione e condivisione.

In conclusione, parrebbe imporsi la necessità di un nuovo quadro giuridico che favorisca sì la continua innovazione e la relativa crescita economica, ma che prevenga altresì le derive peggiori che la digitalizzazione sta producendo, in particolare nel settore dei servizi finanziari.

4. L'I.A. come vittima di reati.

Un'ultima prospettiva di intersezione tra gli sviluppi dell'intelligenza artificiale e il novero dei reati "comuni" è quello che vede l'I.A. quale vittima del reato: o, meglio, quale *oggetto materiale* del reato.

È una prospettiva complessa e cangiante, che vede coinvolti titoli di reato diversi in base alla tipologia di soggetto artificiale che è coinvolto.

Il caso più semplice e già attuale è quello di intelligenze artificiali di tipo non robotico, non dotate cioè di un corpo fisico immediato (salvo cioè il supporto informatico materiale in cui il soggetto in questione è memorizzato). Si tratta, in altre parole, di intelligenze artificiali-programmi informatici, che possano interagire in rete con utenti umani o altri soggetti "informatici".

La tipologia delittuosa di cui tali soggetti artificiali possono essere bersaglio, evidentemente, è quella del *cybercrime*. Resta da capire che cosa aggiunga, rispetto alla fenomenologia più tradizionale, il carattere "intelligente" di simili soggetti. Già le fattispecie esistenti di accesso abusivo a sistema informatico (art. 615-*ter* c.p.), danneggiamento informatico (artt. 635-*bis*, *ter*, *quater*, *quinquies* c.p.) e frode informatica (art. 640 *ter* c.p.) sembrano tutelare tali I.A. da aggressioni di questo tipo. Più in generale, si può notare come una simile tutela prescinda del tutto da un carattere più o meno "intelligente" degli oggetti materiali attinti, appuntandosi su beni da proteggere che sono sì a carattere informatico (riservatezza informatica, ecc.) ma che costituiscono comunque la proiezione di interessi personalistici e/o patrimonialistici di utenti *umani*. Il carattere "intelligente" dei programmi in questione, se probabilmente non merita (ancora) una tutela più incisiva, può forse suggerire la necessità di una tutela rafforzata in ragione della maggiore attitudine di offesa.

L'altra ipotesi, forse più futuristica che attuale, ma di cui già si parla in letteratura, è quella che prende in considerazione soggetti artificiali intelligenti a carattere robotico, dotati cioè di un corpo fisico, in particolare quando questo sia antropomorfo. In tale caso, se non si può probabilmente ancora iniziare a pensare al robot come bene meritevole di tutela di per sé – come già si sta iniziando a proporre in altri campi della tutela penale riguardanti soggetti non umani, come gli animali – già ora si potrebbe invece iniziare a teorizzare la necessità di introdurre nell'ordinamento una qualche forma di tutela mutuata proprio sul modello del "sentimento per".

5. L'intelligenza artificiale ed il contrasto alla pedopornografia.

Come noto, la pedopornografia ha nella rete *internet* (e, più precisamente, nel *dark web*) il suo mezzo privilegiato di diffusione.

L'impiego di sistemi di A.I. nell'attività di *law enforcement* in questo settore è già una realtà, e si presenta in crescita per i prossimi anni.

È il caso delle *chatbot* (sistemi costituiti da rete Seq2seq, che prende in *input* una sequenza di parole e genera in *output* un'altra sequenza di parole) utilizzate per assumere infinite identità al fine di chattare con utenti diversi, contribuendo alla

scoperta di reati di pedopornografia. Sono innegabili, in questa materia, i profili critici quanto alla valenza probatoria e alla disciplina delle attività sotto copertura.

Nell'ambito del gruppo di lavoro – grazie ad una rimarchevole iniziativa del Servizio di Polizia Postale e delle Comunicazioni in collaborazione con l'Università di Bari – sono allo studio le implicazioni giuridiche conseguenti allo sviluppo di un sistema che, sfruttando le tecnologie proprie dell'Intelligenza Artificiale, permetta di sostituire/supportare l'operatore umano nella fase di monitoraggio del *web*. Tale sistema avrebbe il vantaggio di automatizzare le attività di riconoscimento dei siti *web* di natura pedopornografica – oggi molto onerose in termini di uomini e mezzi – e di velocizzare i processi di categorizzazione del materiale pedopornografico detenuto, supportando le operazioni di perquisizione informatica.

Oltre a rendere più efficace l'attività di analisi di ingente materiale, il *software* eviterebbe la traumatica esposizione dell'operatore alla visione del materiale pedopornografico, limitando il ruolo di quest'ultimo alla semplice valutazione finale di genuinità della categorizzazione.

Al fine di poter utilizzare gli strumenti e i metodi della Intelligenza Artificiale, gli algoritmi di *machine learning* hanno tuttavia necessità di un addestramento specifico, basato sull'analisi di *dataset* di foto pedopornografiche.

È in fase di studio la corretta procedura che autorizzi al trattamento di immagini pedopornografiche per finalità di ricerca, per il periodo temporale strettamente necessario all'addestramento dell'algoritmo.