Fondazione Vittorio Occorsio

CRIMINALITÀ INFORMATICA E INTELLIGENZA ARTIFICIALE

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

II/2022

SOMMARIO

Premessa

di Eugenio Occorsio*

Se oggi mio padre, con una visione favolistica scritta con i toni di Antoine de Saint-Exupery, tornasse per un giorno sulla Terra, sarebbe felice di rivederci, di conoscere mio figlio che porta il suo nome, ma soprattutto sarebbe piacevolmente stupito. Intanto vedendo che esiste una Fondazione a lui intestata, Vittorio Occorsio, nata per onorare la sua memoria e per valorizzare i suoi metodi di indagine. Poi avrebbe un moto di tenerezza pari alla stima e alla simpatia (reciproca) che nutriva verso le insostituibili forze di polizia con le quali ha lavorato per tanti anni, insegnando anche in diverse scuole di perfezionamento fra Polizia di Stato (che allora si chiamava con le stesse iniziali "pubblica sicurezza") e Arma dei Carabinieri. Infine si chiederebbe, ci chiederebbe, di spiegargli il titolo stesso di questo corso e del volume che lo presenta. Mio padre è morto nel 1976 e, come si dice ed è vero, in questo quasi mezzo secolo lo sviluppo tecnologico ha fatto tanti passi avanti quanto nei dieci secoli precedenti. "Criminalità informatica" è un termine che sì, forse esisteva ma era un'entità ancora indistinta, limitata a qualche caso di spionaggio internazionale, certo non centrale com'è divenuto oggi ad ogni livello. Quanto a "intelligenza artificiale", era abbastanza impegnato a spremere la sua di "intelligenza naturale" che certo non avrebbe mai pensato che in un giorno neanche così lontano, nell'arco di una generazione (la mia), si sarebbe arrivati a picchi di tale sofisticata potenza. Addirittura, è cronaca di queste settimane, al software che scrive testi, giudica, esprime opinioni (che poi ci sia chi di queste opinioni si fida è un altro discorso).

Certo, è inevitabile riflettere sul fatto che mio padre affrontava e spesso risolveva, così come tutti i magistrati e le forze di polizia di allora, casi complessi e trame intricate senza le banche dati, senza Internet, senza appunto l'intelligenza artificiale. Ma oggi che c'è, diciamo per fortuna purché si tengano presenti i pericoli dell'uso improprio (ma questo magistrati e forze dell'ordine lo sanno benissimo), è importante conoscerla a fondo e soprattutto valutare il contributo che l'IA, come viene ormai confidenzialmente chiamata, può dare alle indagini, alle ricerche, perfino alle tanto vituperate quanto indispensabili intercettazioni (non c'erano neanche queste se non in misura ridottissima ai tempi di mio padre).

(*) Giornalista e scrittore, fondatore della Fondazione Vittorio Occorsio.

Perciò è meritoria quest'iniziativa che, con l'egida della Fondazione Vittorio Occorsio, sta prendendo vita con un corso a mio padre intitolato. Sarebbe lungo l'elenco dei ringraziamenti: il direttore della Scuola di Perfezionamento Generale Giuseppe La Gala, i magistrati Giovanni Salvi e Pasquale Fimiani ai quali tanto la Fondazione deve, la professoressa Carmela Decaro che tanto affettuosamente ci segue fin dall'inizio con grande dispendio personale di energie, fino a coloro che hanno raccolto e ordinato gli atti di questo quaderno. A tutti – scusandomi per le dimenticanze – va il ringraziamento della nostra famiglia, e a tutti il miglior augurio di buon lavoro.

La giurisdizione, la questione del *cyberspace* e della sovranità digitale europea

di Giovanni Salvi*

Vittorio Occorsio fu assassinato il 10 luglio 1976 da Pierluigi Concutelli, dirigente di Ordine Nuovo, a quel tempo collegato anche con l'organizzazione Avanguardia Nazionale, al cui vertice era Stefano Delle Chiaie.

La storia umana e professionale di Occorsio è emblematica di una radicale trasformazione nel ruolo della magistratura, che fu a sua volta determinata dal peso della gravissima minaccia per la stabilità democratica del Paese, sotto la pressione contemporanea del terrorismo e della criminalità mafiosa.

Gli anni '70 si aprono con la strage del 12 dicembre 1969 e con la incombente minaccia di un colpo di Stato, quel "tintinnare di sciabole" che costituiva un'ipoteca su ogni prospettiva di rinnovamento. Decennio lungo, che prosegue con le stragi indiscriminate e non rivendicate, ormai attribuite con certezza a un disegno destabilizzante nel quale un ruolo determinante ebbero le organizzazioni di estrema destra, e si conclude idealmente con l'omicidio, il 23 giugno, di Mario Amato, che anticipa la strage di Bologna del 2 agosto 1980. In questo decennio esplodono le tensioni sociali e si impongono le organizzazioni eversive di estrema sinistra.

Contemporaneamente, fenomeni di criminalità particolarmente aggressivi, come i sequestri di persona, si diffondono e contribuiscono a rafforzare le organizzazioni criminali. Le guerre di mafia rendono evidente la gravità della minaccia mafiosa e costituiscono il preludio agli omicidi eccellenti della fine del decennio e dei primi anni '80.

Vittorio Occorsio è al crocevia di queste dinamiche. È un magistrato moderato e schivo, ma di tempra forte e non condizionabile, come dimostrerà, alla fine degli anni sessanta, quando verrà incaricato di sostenere l'accusa nello storico processo per diffamazione, intentato dal generale De Lorenzo nei confronti dei giornalisti Eugenio Scalfari e Lino Jannuzzi, che avevano rivelato l'esistenza del Piano Solo del SIFAR e di un dossieraggio politico. Opposto dal Governo il segreto di Stato, Occorsio si convince che al fondo degli articoli dei due giornalisti vi è molto di vero e ne chiede l'assoluzione. Il comportamento indipendente del magistrato comporterà una reazione del vertice del SIFAR. Il generale De Lorenzo scriverà riservatamente al Procu-

(*) Già Procuratore Generale presso la Corte di Cassazione.

ratore Capo, protestando contro un p.m. irrispettoso.

L'esperienza del processo servirà a Occorsio per orientarsi quando gli verrà affidata l'indagine sugli attentati del 12 dicembre di Roma e Milano. Egli si convincerà della responsabilità di Pietro Valpreda e ne chiederà il rinvio a giudizio, attirandosi le polemiche di chi invece riteneva l'imputato innocente e vittima di macchinazioni, ma al contempo individuerà la presenza nel Circolo anarchico di Valpreda di militanti legati all'avanguardista Stefano Delle Chiaie, a sua volta coinvolto nella preparazione di un colpo di Stato, nella notte dell'Immacolata del 1970.

Con questo patrimonio di esperienza affronta le indagini su Ordine Nuovo per ricostituzione del Partito Fascista. Ottiene la condanna degli organizzatori, che porta allo scioglimento dell'organizzazione, per ordine del Ministero dell'Interno.

Nello stesso tempo, Occorsio indaga sui sequestri di persona, con altri magistrati, in uno dei primi gruppi di lavoro degli inquirenti. Qui, individua i legami tra organizzazioni criminali, anche di stampo mafioso, e Ordine Nuovo. Queste indagini porteranno Occorsio a chiedere la cattura di un importante legale, accusato – poi, però, prosciolto – di avere riciclato un'ingente somma di denaro proveniente da un sequestro di persona. Quell'avvocato risulterà essere segretario di una Loggia massonica, la P2.

Occorsio è dunque arrivato, il 7 aprile 1976, tre mesi prima del suo assassinio, alle porte del legame tra criminalità organizzata, terrorismo e logge massoniche occulte.

A questi risultati il magistrato era giunto perché non si era acquietato nell'utilizzo delle categorie interpretative correnti. Egli aveva approfondito le origini dei movimenti eversivi di cui si occupava, studiandone le fondamenta ideali. Aveva compreso che la categoria che voleva l'estremismo di destra come un supporto, per quanto malinteso, di uno Stato impegnato nel contrasto della "minaccia comunista" era inadeguata a comprendere le profonde trasformazioni dell'eversione di destra. Colse, quindi, la grande pericolosità dell'organizzazione Ordine Nuovo.

Così come aveva operato, insieme ad altri colleghi, in maniera innovativa sui sequestri di persona, modificò il suo approccio investigativo e in breve tempo arrivò alla inquisizione dei principali attori di questo movimento, che a seguito delle sue indagini fu sciolto. Era la prima volta che si verificava lo scioglimento di un'organizzazione volta alla ricostituzione del partito fascista.

La lezione della vita professionale di Vittorio Occorsio è che il metodo investigativo deve cambiare a seconda del suo oggetto: non è possibile utiliz-

zare lo stesso strumento investigativo per investigare oggetti diversi. Questa è la linea di pensiero che ci ha portato a lavorare sul tema dell'intelligenza artificiale applicata al processo penale. Tema ampiamente arato e sviluppato, se ne occupano in tanti. La Fondazione Vittorio Occorsio intende però occuparsi di una nicchia molto particolare. Ci interroghiamo, dunque, su come l'impiego di tecnologie avanzatissime (ancora di più in futuro) trasformi innanzitutto l'elemento oggettivo del reato, delineando al tempo stesso condotte nuove, meritevoli della sanzione penale.

Cambia anche l'elemento soggettivo del reato, ponendo problemi di difficile soluzione nel rapporto tra l'azione umana e quella sempre più autonoma della macchina.

L'IA è al contempo anche un potente strumento di investigazione, che richiede conoscenze tecniche approfondite e la capacità di adeguare lo strumento all'oggetto della investigazione.

La nostra quindi è una nicchia. Essa non riguarda aspetti già molto esplorati degli effetti della IA sul modo di affrontare la giurisdizione, ad esempio nell'organizzazione degli uffici o nel fornire supporto al giudice nella decisione; le questioni, molto serie, della non neutralità dell'IA, ad esempio perché utilizzante algoritmi riproducenti e rafforzanti i pregiudizi, sono state ampiamente discusse anche nelle aule di giustizia, prima negli Stati Uniti e ormai anche nel nostro Paese.

Molto meno esplorati sono i temi dei riflessi sostanziali dell'impiego della IA nelle condotte illecite e di conseguenza anche delle sue potenzialità a fini investigativi. Si tratta dunque di diffondere questa consapevolezza tra gli operatori del diritto.

Quando si parla di IA, nel contesto appena delineato, ci si riferisce al rapporto che si determina tra la capacità della macchina di apprendere e la sua capacità di rispondere immediatamente ed autonomamente secondo programmi, previsti anticipatamente ma che si evolvono attraverso l'apprendimento ad opera della macchina stessa. Questo processo avviene in continuazione, interagisce con altre informazioni e può far sì che la macchina, se abilitata, assuma determinazioni autonome sulla base dell'apprendimento.

Tale meccanismo ha importanti riflessi sulla struttura dei reati. Si consideri la manipolazione del mercato finanziario; la manipolazione del mercato attraverso l'impiego di strumenti di IA è diversa da quella che può fare il soggetto umano. Essa risponde a logiche che non sono causali, come noi siamo abituati a pensare, ma che sono meramente probabilistiche, e che solo un'enorme capacità di calcolo riesce poi a trasformate in azioni che hanno efficacia operativa. Questo determina un'estrema difficoltà di prevenirle e di reagi-

re. Ciò pone il tema della responsabilità dell'individuo e di quella dell'ente, o meglio della macchina, e dei rapporti tra le due forme di responsabilità

Vi è tuttavia un ulteriore aspetto che attiene all'esercizio della giurisdizione e che è forse l'elemento di maggiore novità, talmente significativo da far sì che la stessa prospettiva di una utile risposta in sede di giustizia penale divenga problematica.

La estrema rapidità, la volatilità, la non localizzazione dei vari frammenti della condotta determina l'inefficacia dell'*enforcement* della giurisdizione. Si badi bene, non della affermazione della giurisdizione, che qualunque Stato può rivendicare senza alcun problema nei rapporti con la comunità internazionale, ma delle azioni che la rendono effettiva e che vengono in urto con l'affermazione della sovranità di atri Stati, con altre giurisdizioni. A questa difficoltà cerca di reagire la convenzione di Budapest, soprattutto con il Secondo Protocollo Aggiuntivo, aperto alla firma e già sottoscritto dall'Italia. Nella stessa direzione va il pacchetto della *e-evidence*, in fase di approvazione da parte dell'Unione europea.

Tuttavia, la realizzazione effettiva di questo cambiamento totale di paradigma dei rapporti internazionali non sarà facile da attuare perché richiede una mutua fiducia tra gli Stati che va aldilà dell'UE, e anche del Consiglio d'Europa. Reagire prima di ottenere il consenso dello Stato presso il quale si deve intervenire implica la fiducia tra gli Stati e tra gli organi investigativi. La Convenzione di Budapest cerca di realizzare questo obiettivo, nel suo Protocollo aggiuntivo, attraverso la stabilizzazione delle squadre comuni; esse divengono sostanzialmente un modo per superare il problema del consenso. Si spera che questo meccanismo possa essere efficace, ma è necessario interrogarsi su come esso possa operare nei vari temi specifici di cui parliamo oggi. La questione dell'*enforcement* della giurisdizione si collega a quella di cui ci parlerà il Ten. Col. Signoretti, già ricercatore presso il NATO Cooperative Cyber Defence Centre of Excellence, centro promotore del progetto del Manuale di Tallinn[1], che costituisce il riferimento a livello internazionale nella materia che ci occupa. Nell'ambito del diritto pubblico internazionale, i problemi che gli Stati devono affrontare, infatti, non sono diversi da quelli delle giurisdizioni nazionali. Si pensi al tema della attribuzione, cioè ai criteri

1) Il *Tallinn Manual Project* è un progetto di ricerca del NATO Cooperative Cyber Defence Centre of Excellence (CDCOE) di Tallinn (Estonia). I prodotti dell'attività di ricerca – avviata nel 2009 su iniziativa del NATO CDCOE – sono stati il *Tallinn Manual on the international law applicable to cyber warfare* (2013) e il *Tallinn Manual on the International law applicable to cyber operations* (2017). Gli autori del Tallinn Manual sono un Gruppo di Esperti Internazionali invitati dal Centro e il Direttore ed Editore è il Prof. Micheal N. Schmitt. Il Manuale di Tallinn è proprietà della Cambridge University Press.

di imputazione di una condotta, ad esempio un grave attacco alle strutture informatiche di un Paese, ad una specifica Nazione, secondo parametri accettati nei rapporti tra Stati; problemi analoghi si pongono per la reazione ad attacchi esterni, la cui legittimità riposa, oltre che sulla "attribuzione", anche sulla sussistenza dei presupposti della *self-defence*. Oppure, infine, si pensi alla complessità dell'accertamento delle condizioni che consentono di affermare la responsabilità degli Stati sulla base del principio della due-diligence, per gli Stati che non abbiano agito intenzionalmente. Questi aspetti sono affrontati dalla dr.ssa Nunzia Ciardi, già direttore della Polizia Postale e delle Comunicazioni, e dal 16 settembre vice direttore generale dell'Agenzia per la Cybersicurezza Nazionale.

Laura Carpini, direttrice Unità *Cyber* del Ministero degli Affari Esteri e della Cooperazione Economica e responsabile per il nostro Paese nel working group delle Nazioni Unite per il raggiungimento di un'idea condivisa di spazio virtuale, ci parlerà delle diverse visioni esistenti nella Comunità internazionale dello spazio virtuale. L'Italia ritiene che anche in tale ambiente, nel cyberspace, si applichino i principi del diritto internazionale pubblico, conclusione alla quale è giunto il Manuale Tallinn 2.0. Da visioni diverse derivano conseguenze, non tutte ancora a noi chiare.

Le giornate proseguiranno affrontando diversi aspetti che abbiamo individuato nel tempo attraverso i gruppi di lavoro della FVO e attraverso l'apporto della Procura Generale della Cassazione.

II dr. Fimiani darà conto di alcuni arresti giurisprudenziali, anche a livello europeo, che sono di particolare importanza per affrontare questi argomenti.

I paradigmi essenziali delle indagini che impiegano tecnologie informatiche avanzate saranno illustrate dal Procuratore Aggiunto di Milano, dr. Eugenio Fusco, che voi conoscete tutti perché da tanti anni impegnato in questo settore.

Passeremo poi ad esaminare, con l'aiuto di esperti, di magistrati e di funzionari delle varie Forze di polizia, come il Col. Gianluca Berruti e il prof. Ivan Salvadori, alcune tematiche specifiche, in cui l'IA si manifesta con maggiore rilevanza, o nella trasformazione del reato o perché costituisce una nuova opportunità investigativa. Tra le quali, la manipolazione dei mercati finanziari, in questi giorni particolarmente interessante visto il crollo di alcune monete virtuali.

Particolarmente ampio il contributo del dr. Fabio Di Vizio e dei professori Francesco Bruschi e Vincenzo Rana sul tema degli *asset* virtuali. È necessario conoscerne approfonditamente i meccanismi di funzionamento.

Essi infatti costituiscono insieme una grande opportunità di sviluppo delle transazioni legali e al tempo stesso un'opportunità per attività illecite, delle quali il riciclaggio costituisce solo una parte. L'aspetto finanziario si lega in generale all'utilizzo di monete/*assets* virtuali ai fini di riciclaggio; quindi avremo anche un approfondito esame di questi aspetti. Di per sé il *virtual coin* non solo non è illegale, ma è parte del nostro futuro. Le nuove tecnologie di scambio di valori però introducono elementi di estrema difficoltà per la individuazione dei movimenti soprattutto quando essi si svolgono interamente al di fuori dell'area regolamentata. Anche dal punto di vista delle indagini e degli strumenti di cui si dispone, l'esame degli *asset virtuali* costituisce un settore di straordinario interesse. Attraverso le esperienze sul campo e con l'aiuto di esperti, saranno affrontati sia gli aspetti di carattere generale che quelli specifici, imposti dalle indagini in ambiente virtuale, come ad esempio le procedure tecniche che consentono il sequestro di beni virtuali. Questi aspetti saranno illustrati anche attraverso un'esperienza di laboratorio.

Un'altra questione molto interessante è quella relativa alla manipolazione del mercato politico. La manipolazione, la disinformazione, sono sempre stati uno strumento della lotta politica e delle interferenze tra Stati (si pensi all'alterazione delle immagini nei regimi autoritari o alla redazione dei Protocolli dei Savi di Sion, falso costruito dai Servizi dello Zar e ancora utilizzato nelle polemiche antiebraiche nonostante ne sia nota l'origine). Tuttavia, l'IA moltiplica queste potenzialità, le rende estremamente difficili da individuare e da contrastare. Ciò finisce per minare un elemento comune a tutti gli ordinamenti democratici, la fiducia nello spazio pubblico come elemento essenziale di coesione di una società democratica. È dunque necessario che la fiducia nello spazio pubblico sia difesa dalle aggressioni. Ma questa tutela può prevedere anche la sanzione penale? Ed entro quali limiti, vista la rilevanza degli interessi costituzionali in gioco e in bilanciamento, come ad esempio il diritto di organizzarsi per concorrere alla vita politica o quello di manifestare liberamente il proprio pensiero.

L'ultimo degli argomenti proposto apre prospettive innovative: l'impiego dell'intelligenza artificiale per la tutela dell'ambiente.

Qui non si tratta tanto del fatto che i reati vengono trasformati, quanto che le nuove tecnologie forniscono nuove potenzialità di indagine sui reati transnazionali in materia di ambiente. La possibilità di utilizzare un numero enorme di informazioni aperte, unite alle informazioni riservate (la c.d. teoria del mosaico), può dare la possibilità di indentificare con precisione il luogo di provenienza di un grande inquinamento di acque internazionali, può dare la possibilità di individuare i traffici di rifiuti altamente pericolosi e quindi ri-

costruirne la provenienza. L'impiego di queste tecnologie può probabilmente cambiare il nostro modo di lavorare in questa materia.

Di questo ci parlerà un gruppo di esperti di alto livello, tra cui ancora una volta Pasquale Fimiani che è il referente della rete europea dei procuratori generali in materia di tutela dell'ambiente. Vi ringrazio molto per l'opportunità che ci date per testare se stiamo andando sulla strada giusta. Il ritorno che ci darete è molto importante per la FVO, ma ancor di più per l'efficacia della risposta giurisdizionale.

Mi auguro che queste esperienze si diffondano nella polizia giudiziaria e tra i magistrati del p.m., anche grazie agli atti del seminario, oggi pubblicati sulla prestigiosa rivista della Scuola Interforze, volume curato da Alberto Cappellini e Ivan Salvadori, cui va il nostro ringraziamento.

Principi fondamentali nella giurisprudenza nazionale e sovranazionale

di Pasquale Fimiani*

Nella presentazione del Corso sono enunciati i due temi oggetto di approfondimento: i reati informatici in senso stretto (quelli nei quali l'elemento tecnologico è indispensabile per la stessa configurabilità) e l'uso di strumenti informatici per la commissione di reati comuni (ambito nel quale un focus particolare è destinato all'intelligenza artificiale nell'illecito penale).

Propedeutici all'esame di questi argomenti sono due temi trasversali.

Il primo è rappresentato dal concetto di *sistema informatico* o *telematico*, indicato quale oggetto di tutela diretta[1] e richiamato da diverse fattispecie di reato[2].

L'art. 1 della Convenzione europea di Budapest del 23 novembre 2001 definisce sistema informatico "*qualsiasi apparecchiature o gruppi di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica dei dati*".

Il Legislatore non definisce il "sistema informatico o telematico" e la nozione deve essere tratta dalla prassi e dalle conoscenze tecniche attuali.

La Cassazione ha affermato che per sistema informatico si deve intendere «*un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate – per mezzo di un'attività di "codificazione" e "de–codificazione" – dalla "registrazione" o "memorizzazione", per mezzo di impulsi elettronici, su supporti adeguati, di "dati", cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit), in combinazione diverse, e dalla elaborazione automatica di tali dati, in modo*

(*) Avvocato generale della Corte di Cassazione, Componente del Comitato Scientifico FVO.

1) Reati di cui agli artt. 615-*ter* c.p. (accesso abusivo ad un sistema informatico o telematico), 615-*quater* c.p. (detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici), 615-*quinquies* c.p. (detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico) e 635-*quinquies* c.p. (danneggiamento di sistemi informatici o telematici di pubblica utilità).

2) Reati di cui agli artt. 392 c.p. (esercizio arbitrario delle proprie ragioni con violenza sulle cose), 617-*quater* c.p. (intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche), 617-*quinquies* c.p. (detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche), 617-*sexies* c.p. (falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche), 640-*ter* c.p. (frode informatica).

da generare "informazioni", costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente»[3].

Tale definizione è coerente con quella di "*sistema informativo*" presente nell'art. 1 del d.P.C.M. 30 luglio 2020 n. 131 (Regolamento in materia di perimetro di sicurezza nazionale cibernetica) quale dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati digitali, ivi inclusi i sistemi di controllo industriale.

La sua ampiezza consente includere tutti i sistemi capaci di trattare in modo automatizzato dati, quali quelli relativi al funzionamento delle carte di pagamento[4], ovvero quelli di videosorveglianza[5].

Quanto ai sistemi telematici, si è affermato che "la telematica poi altro non è che l'applicazione dell'informatica alle tecnologie della comunicazione", con la conseguenza che «un sistema telematico si basa sulla connessione in rete, aperta (Internet) o chiusa (per es. una "Local Area Network" o "LAN", separata dalla rete pubblica tramite firewall, ovvero una "Virtual Private Network" o "VPN", in cui i dati sono trasmessi crittografati e dunque in modalità sicura) tra sistemi informatici: in tal caso è possibile sia l'elaborazione, che la trasmissione a distanza di dati e informazioni, ivi inclusi suoni, voci, immagini o video (per es. la rete televisiva o quella per telefoni fissi e/o per cellulari, una centralina

---

3) Cass. pen., sez. un., 24 aprile 2015, n. 17325 (e successive conformi). Sulla base di tale definizione, la S.C. ha affermato che, in tema di acceso abusivo ad un sistema informatico o telematico, il luogo di consumazione del delitto di cui all'art. 615-*ter* c.p. coincide con quello in cui si trova l'utente che, tramite elaboratore elettronico o altro dispositivo per il trattamento automatico dei dati, digitando la "parola chiave" o altrimenti eseguendo la procedura di autenticazione, supera le misure di sicurezza apposte dal titolare per selezionare gli accessi e per tutelare la banca-dati memorizzata all'interno del sistema centrale ovvero vi si mantiene eccedendo i limiti dell'autorizzazione ricevuta (in motivazione la Corte ha specificato che il sistema telematico per il trattamento dei dati condivisi tra più postazioni è unitario e, per la sua capacità di rendere disponibili le informazioni in condizioni di parità a tutti gli utenti abilitati, assume rilevanza il luogo di ubicazione della postazione remota dalla quale avviene l'accesso e non invece il luogo in cui si trova l'elaboratore centrale).

4) Cass. pen., sez. fer., 12 novembre 2012, n. 43755, per la quale integra il reato di accesso abusivo ad un sistema informatico la condotta di chi si introduce nel sistema POS predisposto per il pagamento a mezzo carte di credito e bancomat, installando un "microchip" idoneo ad intercettare le comunicazioni informatiche di detto apparato e a scaricarne i dati, per poi successivamente utilizzarli al fine di clonare altre carte (nella specie, la S.C. ha precisato, richiamando le definizioni contenute nella Convenzione di Budapest del 23 novembre 2001, che le carte di credito, essendo idonee a trasmettere dati informatici, costituiscono un vero e proprio sistema informatico nel momento in cui si connettono all'apparecchiatura POS).

5) In quanto composto di videocamere che non solo registrano le immagini, trasformandole in dati memorizzati e trasmessi ad altra componente del sistema secondo un programma informatico – attribuendo alle predette immagini la data e l'orario e consentendone la scansione in fotogrammi – ma si avvale anche di un hard disk che riceve e memorizza tutte le immagini, rendendole estraibili e riproducibili per fotogrammi (Cass. pen., sez. II, 14 marzo 2012, n. 9870).

telefonica, reti "ADSL" o a fibre ottiche, sistemi "VOIP")»[6].

Sono "di interesse pubblico" (condizione per la configurabilità dell'aggravante di cui all'art. 615-*ter*, comma 3, c.p.) solo i sistemi informatici o telematici di pubblica utilità, ossia destinati al servizio di una collettività indifferenziata e indeterminata di soggetti, e non anche quelli a vario titolo riconducibili all'esercizio di diritti, pur di rilevanza collettiva, costituzionalmente tutelati[7].

Quanto alla nozione di operatore del sistema (prevista, nel caso di abuso di tale qualità, come circostanza aggravante dall'art. 615-*ter*, comma 2, n. 1 c.p. e dall'art. 617-*quater*, comma 2, n. 2, c.p.), riveste siffatta qualifica non solo il titolare di poteri decisori sulla gestione dei contenuti o sulla configurazione del sistema, ma anche colui che, pur se destinato a svolgere compiti meramente esecutivi, sia comunque abilitato a operare sul sistema, modificandone i contenuti o la struttura[8].

Le Sezioni Unite hanno poi affermato che integra il delitto previsto dall'art. 615-*ter*, secondo comma, n. 1, c.p. la condotta del pubblico ufficiale o dell'incaricato di un pubblico servizio che, pur essendo abilitato e pur non violando le prescrizioni formali impartite dal titolare di un sistema informatico o telematico protetto per delimitarne l'accesso, acceda o si mantenga nel sistema per ragioni ontologicamente estranee rispetto a quelle per le quali la facoltà di accesso gli è attribuita[9].

La seconda questione di carattere generale utile per la comprensione dei temi oggetto del corso è quella della *responsabilità degli internet service provider per i contenuti illeciti pubblicati da terzi.*

L'internet hosting provider è definito dal d.lgs. n. 70 del 2003, art. 16 come colui che si limita a prestare un "servizio consistente nella memorizzazione di informazioni fornite da un destinatario del servizio"[10]. Da

---

6) Bassoli, *I crimini informatici, il dark web e le web room*, Pacini giur., 2021, 131.
7) Cass. pen., sez. V, 23 giugno 2021, n. 24576 (fattispecie in cui la Corte ha escluso la sussistenza dell'aggravante nel caso di accesso abusivo al sito del fondatore di un movimento politico di livello nazionale utilizzato per la divulgazione delle idee di detto movimento).
8) Cass. pen., sez. V, 3 marzo 2022, n. 7775, che ha definitivamente superato l'assunto secondo cui per "operatore del sistema" debba intendersi qualunque soggetto il quale, autorizzato all'accesso al sistema informatico, abusi di detta autorizzazione (interpretazione estensiva, in grado di ricomprendere anche il mero utente che fruisce dei contenuti presenti nel sistema informatico, seguita in precedenza dalla S.C.).
9) Cass. pen., sez. un., 8 settembre 2017, n. 41210 (nella specie, la S.C. ha ritenuto immune da censure la condanna di un funzionario di cancelleria, il quale, sebbene legittimato ad accedere al Registro informatizzato delle notizie di reato – c.d. Re.Ge. – conformemente alle disposizioni organizzative della Procura della Repubblica presso cui prestava servizio, aveva preso visione dei dati relativi ad un procedimento penale per ragioni estranee allo svolgimento delle proprie funzioni, in tal modo realizzando un'ipotesi di sviamento di potere).
10) Per questa ragione è «palese l'intrinseca diversità tra gli internet providers e gli amministratori

tale definizione, interpretata nel contesto complessivo dello stesso art. 16, emerge, infatti, che il gestore del servizio di hosting non ha alcun controllo sui dati memorizzati, né contribuisce in alcun modo alla loro scelta, alla loro ricerca o alla formazione del file che li contiene, essendo tali dati interamente ascrivibili all'utente destinatario del servizio che li carica sulla piattaforma messa a sua disposizione. A tale proposito, risulta significativo che, secondo l'espressa previsione dello stesso art. 16, lo hosting provider non sia responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio[11].

E ciò, alla duplice condizione: che il provider non sia effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illiceità dell'attività o dell'informazione; che, non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso. Così disponendo, in conformità della direttiva 2000/31/CE, il legislatore ha inteso porre quali presupposti della responsabilità del provider proprio la sua effettiva conoscenza dei dati immessi dall'utente e l'eventuale inerzia nella rimozione delle informazioni da lui conosciute come illecite[12].

Va però tenuto presente che sono ormai da tempo in uso tecnologie di filtraggio preventivo idonee ad identificare automaticamente i contenuti even-

---

di blog, dal momento che questi ultimi non forniscono alcun servizio nel senso precisato, bensì si limitano a mettere a disposizione degli utenti una piattaforma sulla quale poter interagire attraverso la pubblicazione di contenuti e commenti su temi nella maggior parte dei casi proposti dallo stesso blogger, in quanto caratterizzati dalla linea, che si potrebbe definire (anche se impropriamente) "editoriale", impressa proprio dal gestore della suddetta piattaforma» (Cass. pen., sez. V, 20 marzo 2019, n. 12546).

11) Vedi anche Corte di giustizia 23 marzo 2010, procedimenti da C-236/08 a C-238/08 (punto 120), nella quale si afferma che l'art. 14 della Direttiva sul commercio elettronico (corrispondente al d.lgs. n. 70 del 2003, art. 16) deve essere interpretato nel senso che si applica al prestatore di un servizio di posizionamento su Internet qualora detto prestatore non abbia svolto un ruolo attivo a conferire la conoscenza o il controllo dei dati memorizzati. Se non ha svolto un tale ruolo, il provider non può essere ritenuto responsabile per i dati che ha memorizzato, salvo che, essendo venuto a conoscenza della natura illecita di tali dati, abbia omesso di prontamente rimuoverli o di disabilitare l'accesso agli stessi.

12) Considerazioni tratte dalla motivazione di Cass. pen., sez. III, 3 febbraio 2014, n. 5107, secondo cui «non è configurabile il reato di trattamento illecito di dati personali a carico degli amministratori e dei responsabili di una società fornitrice di servizi di "Internet hosting provider" che memorizza e rende accessibile a terzi un video contenente dati sensibili (nella specie, un disabile ingiuriato e schernito dai compagni in relazione alle sue condizioni), omettendo di informare l'utente che immette il "file" sul sito dell'obbligo di rispettare la legislazione sul trattamento dei dati personali, qualora il contenuto multimediale sia rimosso immediatamente dopo le segnalazioni di altrui utenti e la richiesta della polizia».

tualmente illeciti di un video o di una comunicazione[13].

Si è giustamente osservato[14] che l'internet provider «si affida ad algoritmi di associazione e filtraggio per l'intera selezione dei contenuti mostrati e per la gran parte del controllo di quanto pubblicato, in totale assenza di una mente "umana" a presiedere le attività delle piattaforme o a sorvegliare il comportamento degli utenti. Rimettere il monitoraggio dei contenuti al solo umano, sarebbe, invero, impensabile, essendo costui ontologicamente impossibilitato a svolgere una sorveglianza esauriente a fronte del numero spropositato di utenti attivi ogni minuto sulla rete. Come fare quindi a costruire un modello di responsabilità penale quando progressivamente scompaia l'umano (rimproverabile quantomeno a titolo di colpa) e residui solo la macchina?».

La risposta a tale quesito deve prendere le mosse dal rilievo che non è configurabile a carico dell'internet hosting provider un obbligo giuridico di impedire l'evento collegato alla immissione in rete di contenuti illeciti, in quanto egli ha l'obbligo di rimuoverli solo dopo che ne sia venuto a conoscenza e, quindi, successivamente alla commissione del reato, con la conseguenza che va esclusa una sua posizione di garanzia e non è configurabile una sua responsabilità a titolo di reato omissivo improprio per mancato impedimento dell'evento[15].

Occorre quindi fare riferimento alle regole ordinarie in materia di concorso di persone, la cui tenuta, però, quando il reato commesso dal terzo sia punito solo a titolo di dolo (come nel caso di reti di diffamazione on-line), richiede che anche per l'internet hosting provider sussista lo stesso elemento soggettivo, non essendo configurabile il concorso colposo nel delitto doloso in assenza di una espressa previsione normativa, non ravvisabile nell'art. 113 c.p. che contempla esclusivamente la cooperazione colposa nel delitto colposo[16].

Appare peraltro complesso individuare la stessa condotta colposa, stante l'autonomia dei sistemi di intelligenza artificiale nell'analizzare le informazioni.

La colpa, almeno sotto il profilo teorico, potrebbe in astratto collocarsi

---

13) In questa prospettiva, il c.d. Digital Services Act in Corso di elaborazione a livello eurounitario si propone di emendare la direttiva 2000/31 con l'introduzione di forme più stringenti di controllo da parte del provider.

14) Bassoli, *I crimini informatici*, cit., 197.

15) Per queste ragioni Cass. pen., sez. V, 20 marzo 2019, n. 12546 critica sez. V, 27 dicembre 2016, n. 54946, che ha confermato la responsabilità di un gerente un sito internet, per avervi mantenuto consapevolmente un articolo diffamatorio, per il fatto che la diffamazione è un reato istantaneo mentre l'obbligo d'impedimento sul quale si fondava il giudizio di responsabilità concorsuale, era stato collocato in un momento successivo a quello della consumazione del reato, ed ha proposto, al riguardo, di fare ricorso alla figura della pluralità di reati, integrati dalla ripetuta trasmissione del dato denigratorio.

16) *Ex plurimis*, Cass. pen., sez. IV, 14 febbraio 2019, n. 7032 e sez. V, 18 dicembre 2018, n. 57006.

nella fase di predisposizione degli algoritmi, ma anche in questo caso ne appaiono complessi la configurabilità e l'accertamento.

Sembra quindi più agevolmente configurabile una responsabilità civile[17] specie in considerazione degli obblighi di autonoma attivazione e controllo che in prospettiva saranno previsti in capo all'internet hosting provider, con l'attuazione del c.d. *Digital service act*.

Bibliografia

Anselmi, *Accesso abusivo ad un sistema informatico o telematico e competenza territoriale*, in *Dir. Pen. e Processo*, 2016, 1, 80

Bassoli, *I crimini informatici, il dark web e le web room*, Pacini giur., 2021

Bocchini, *Responsabilità civile dell'hosting provider - La responsabilità civile plurisoggettiva, successiva ed eventuale dell'ISP*, in *Giur. It*., 2019, 12, 2604

Galante, *Accesso abusivo ad un sistema informatico - L'overruling delle Sezioni Unite in tema di accesso abusivo ad un sistema informatico*, in *Giur. It*., 2018, 3, 734

Macrillò, *Punti fermi dlla Cassazione sulla responsabilità dell'internet provider per il reato ex art. 167 d.lgs. n. 196/03*, in *Giur. It*., 2014, 8-9, 2022

Mollo, *La responsabilità del provider alla luce del Digital Service Act*, in *contrattoeimpresaeuropa.eu*, 2 maggio 2022

Pagella, *La Cassazione sulla responsabilità del blogger per contenuti diffamatori (commenti) pubblicati da terzi*, in *penalecontemporaneo.it*, 17 maggio 2019

17) Cfr. Cass. civ., sez. I, 2019, 19 marzo, n. 7708: «Nell'ambito dei servizi della società dell'informazione, la responsabilità dell'"hosting provider", prevista dall'art. 16 del d.lgs. n. 70 del 2003, sussiste in capo al prestatore dei servizi che non abbia provveduto alla immediata rimozione dei contenuti illeciti, oppure abbia continuato a pubblicarli, quando ricorrano congiuntamente le seguenti condizioni: a) sia a conoscenza legale dell'illecito perpetrato dal destinatario del servizio, per averne avuto notizia dal titolare del diritto leso oppure "aliunde"; b) sia ragionevolmente constatabile l'illiceità dell'altrui condotta, onde l'"hosting provider" sia in colpa grave per non averla positivamente riscontrata, alla stregua del grado di diligenza che è ragionevole attendersi da un operatore professionale della rete in un determinato momento storico; c) abbia la possibilità di attivarsi utilmente, in quanto reso edotto in modo sufficientemente specifico dei contenuti illecitamente immessi da rimuovere. Resta affidato al giudice del merito l'accertamento in fatto se, in riferimento al profilo tecnico-informatico, l'identificazione di video, diffusi in violazione dell'altrui diritto, sia possibile mediante l'indicazione del solo nome o titolo della trasmissione da cui sono tratti, oppure sia indispensabile, a tal fine, la comunicazione dell'indirizzo "url", alla stregua delle condizioni esistenti all'epoca dei fatti».

QUESTIONI GENERALI IN TEMA DI ACCERTAMENTO DEI CRIMINI INFORMATICI

di Eugenio Fusco*

Un dato da tener presente:

"*Nel 2021 il costo globale della criminalità informatica ha superato i 600 miliardi di dollari. Un quinto degli attacchi è stato diretto all'Europa*"[1].

1. Premessa

Il fenomeno della criminalità informatica, che si manifesta in forme diverse per perseguire eterogenei obiettivi illeciti, è in crescente espansione.

La rete *internet*, fonte e motore del progresso, è anche e sempre più frequentemente strumento per commettere reati, di qualsiasi genere: buona parte delle fattispecie incriminatrici può essere realizzata informaticamente. Si pensi alla vastissima categoria delle frodi, perpetrate valendosi di piattaforme; in proposito, va ricordato che per costante giurisprudenza è, in questi casi, ipotizzabile la circostanza aggravante ad effetto speciale prevista dall'art. 640, comma 2-*bis*) c.p., che consente, nei casi più gravi e/o a marcata serialità, l'applicazione della misura cautelare (compresa la custodia in carcere) se ricorrono le esigenze di cui all'art. 274 c.p.p.

Ma la rete è anche il mezzo per compiere estorsioni, si pensi a quelle a sfondo sessuale: a Milano siamo riusciti ad identificare un soggetto che si era introdotto nei pc di numerose vittime, tutte ricattate con la minaccia di rendere pubblici dati sensibili inerenti la sfera sessuale; l'estorsore ha utilizzato, ancora la rete, per autoriciclare il profitto del reato, impiegato in operazioni in *bitcoin*.

E si potrebbe proseguire a lungo, poiché, affianco al *numerus calusus* dei reati tipicamente informatici, la gran parte delle fattispecie incriminatrici previste dal codice penale o da leggi penali è stata "metamorfosata dallo strumento informatico".

(*) Procuratore Aggiunto della Repubblica presso il Tribunale di Milano. La presente rielaborazione dell'intervento tenuto al corso tiene conto anche di riflessioni e contributi successivi.

1) Dati forniti dall'a.d. di Leonardo spa al *Cybertech Europe* 2022. Agli attacchi seguono, ma non sempre, forme di riscatto.

2. L'accertamento dei crimini informatici

Nel settore della criminalità informatica, le indagini che si concludono con l'accertamento della responsabilità e l'identificazione dei colpevoli sono scarse, a fronte di quelle, assai più numerose che vengono archiviate: il dato è noto a tutti.

Preoccupano, in particolare, gli attacchi *cyber* alle infrastrutture sensibili, sia per la gravità delle loro conseguenze sia perché, proprio in questo specifico ambito, gli esiti delle indagini non sono affatto soddisfacenti.

Come è stato già detto assai più autorevolmente da chi mi ha preceduto: *le sfide poste dalla criminalità informatica stanno diventando sempre più complesse ed è sempre più difficile affrontarle efficacemente*.

Richiamo anch'io – trovandomi, a mia volta, a svolgere un intervento introduttivo e di carattere generale – la "transnazionalità" e la "delocalizzazione", che rendono arduo il contrasto al fenomeno della criminalità informatica.

Non è escluso che l'estrema difficoltà che si incontra nell'identificazione dei colpevoli, indurrà, in prospettiva, a ragionare su forme di responsabilità a carico degli enti e/o – come già qualcuno ipotizza – delle macchine.

3. La delocalizzazione della criminalità informatica e la necessità di concentrare le indagini per "specializzarle"

Prendendo le mosse dalla "delocalizzazione" dell'azione criminosa, si coglie – come pure è stato anticipato – la "crucialità" del problema della giurisdizione e, a cascata, della competenza per territorio.

Il tema è strettamente connesso – a mio avviso – a quello dell'efficacia dell'azione di contrasto.

L'esperienza maturata in altri (ma contigui) settori dimostra che: *i*) la concentrazione delle indagini presso pochi uffici ha un positivo riflesso sul loro esito; *ii*) ne consegue l'opportunità di ricorrere a criteri di radicamento della competenza incontrovertibili e, in un certo senso, alternativi rispetto a quelli tradizionali.

Mi permetto di prendere spunto da un'esperienza personale, quella maturata, anni addietro, nella materia del *market abuse*.

Grazie all'orientamento giurisprudenziale che fa coincidere la consu-

mazione della manipolazione informativa del mercato con l'immissione della notizia falsa nel server del "Network Information System - NIS" (il sistema che mette a disposizione degli operatori finanziari e dei risparmiatori la notizia), collocato presso la sede della Borsa Valori a Milano, competente a procedere per il reato di aggiotaggio informativo è la Procura di Milano, salvo il caso di connessione con altri più gravi delitti.

La concentrazione delle indagini e dei processi a Milano, oltre ad accumulare una significativa esperienza, sia da parte dei pubblici ministeri che dei giudici, ha anche favorito lo sviluppo di una sempre più stretta collaborazione tra l'Autorità giudiziaria e la Consob: la multifattoriale sinergia che è venuta a crearsi è stata premiante in una materia altamente specialistica[2]. Ricordo quali esempi: il caso Parmalat e l'illegale "scalata" della Popolare di Lodi alla Banca Antonveneta.

Senza voler stabilire graduatorie, anche "il *cyber*" rientra tra le materie specialistiche e richiede, innegabilmente, specifiche professionalità.

La stessa distrettualizzazione della competenza dei reati informatici ne è, in qualche misura, testimonianza; ma non è probabilmente l'opzione più adeguata e, comunque, è insufficiente, se si considera che i reati "distrettualizzati" costituiscono solo una minima parte nella fenomenologia della criminalità informatica.

Occorre partire proprio dalla "delocalizzazione", ricorrente (*rectius*: immanente) nei reati commessi con lo strumento informatico, per perseguire l'obiettivo della concentrazione delle indagini, che – come si è visto – è fattore di miglioramento.

Nell'era di *internet* e della delocalizzazione del crimine, l'inviolabile principio costituzionale del giudice naturale deve essere interpretato evolutivamente.

Sia consentita una digressione che, prendendo spunto dal penale tributario dimostra l'assoluta praticabilità, sul piano giuridico, dell'opzione che s'intende suggerire al Legislatore.

L'art. 18, comma 1 d.lgs. n. 74/2000 detta un criterio suppletivo di determinazione della competenza territoriale, secondo cui: «*Salvo quanto previsto dai commi 2 e 3, se la competenza per territorio per i delitti previsti dal presente decreto non può essere determinata a norma dell'articolo 8 del codice di procedura penale, è competente il giudice del luogo di accertamento del reato*»; viceversa, il comma 2 detta un criterio totalmente derogatorio rispetto alla norma generale di determinazione della competenza territoriale

2) Fusco - Pacini, *Enforcement penale e mercati finanziari nell'era della digitalizzazione*, in *Giurisprudenza Penale*, 07/2022.

(art. 8 c.p.p.), imperniato sul *locus commissi delicti*. È, infatti, stabilito che: «*Per i delitti previsti dal capo I del titolo II il reato si considera consumato nel luogo in cui il contribuente ha il domicilio fiscale. Se il domicilio fiscale è all'estero è competente il giudice del luogo di accertamento del reato*». La *ratio* della disposizione – secondo la Relazione di accompagnamento al d.lgs. – risiede proprio nella volontà di derogare all'applicazione delle regole generali, che darebbero luogo a risultati indesiderabili, stanti le modalità informatiche di trasmissione della dichiarazione fiscale. Infatti, se si avesse riguardo al luogo dal quale la trasmissione è effettuata, l'autore dell'illecito potrebbe scegliersi la competenza territoriale, incaricando della trasmissione un soggetto abilitato operante nel luogo ritenuto più conveniente. Se invece si avesse riguardo al luogo fisico di ricezione della dichiarazione, la competenza risulterebbe attratta in esclusiva al Tribunale di Roma, essendo ivi dislocato il *server* centrale in cui giunge la dichiarazione elettronica. Ecco perché il legislatore ha optato per una disposizione speciale volta a determinare in modo autonomo, per singoli reati, la competenza per territorio. Infatti, il criterio del domicilio fiscale del contribuente è totalmente eccentrico rispetto alla consumazione di un reato di dichiarazione.

La Corte costituzionale ha più volte affermato che la garanzia del giudice naturale è rispettata quando la regola di competenza sia prefissata rispetto all'insorgere della controversia, e non è invece utilizzabile per sindacare la scelta del legislatore che si esprime nella fissazione di quella regola (Corte Cost. ord. n. 68/2009; Corte Cost. ord. n. 138/2008; Corte Cost. ord. n. 193/2003; Corte Cost. ord. n. 417/2002).

Dunque, non osta alcuna ragione giuridica ed è vieppiù auspicabile, con riferimento ai reati commessi a mezzo *internet*, fare perno sul concetto di precostituzione (intesa come previa individuazione per legge[3]) del giudice

3) Giova osservare che tale impostazione è stata ripresa e valorizzata da Cass. S.U. n. 53390/2017, nel chiarire che l'ipotesi di connessione teleologica (art. 12, c. 1, lett. c, c.p.p.) non richiede necessariamente l'identità tra autore del reato-fine e autore del reato mezzo. Si è infatti osservato in motivazione che la diversa opzione «non è d'altro canto imposta, o giustificata, neppure dal rispetto del principio del giudice naturale precostituito per legge, che, secondo tale indirizzo, sarebbe violato se gli autori dei reati meno gravi o, in caso di pari gravità, successivi al primo, fossero attratti nell'orbita della competenza del giudice, rispettivamente, di quello più grave o del primo reato, per la ragione che l'interesse di un imputato alla trattazione unitaria di procedimenti per reati commessi in continuazione, o connessi teleologicamente, non potrebbe pregiudicare quello del coimputato (o dei coimputati) a non essere sottratto al giudice naturale secondo le regole ordinarie della competenza. Tale prospettazione sconta l'adesione alla tradizionale equazione processual-penalistica "giudice naturale = *forum commissi delicti*", trascurando che il valore costituzionalmente tutelato (tra l'altro nel silenzio dell'art. 25 Cost. circa la necessità dell'allocazione del processo nel luogo in cui il reato è stato commesso) è, alla stregua della giurisprudenza costituzionale e di legittimità, quello della imparzialità del giudice, assicurato dalla sua precostituzione rispetto alla vicenda controversa, in base a criteri generali, che, nei

competente, prescindendo dalla "naturalità"; ciò – sia chiaro – non sarebbe in controtendenza rispetto all'esigenza per cui il diritto e la giustizia devono riaffermarsi nel luogo in cui sono stati violati (Corte Cost. ord. n. 168/2006), essendo, piuttosto, la logica conseguenza della inadeguatezza del criterio del *locus commissi delicti*, stabilito dall'art. 8 c.p.p., in un settore penale nel quale – come in altri – l'individuazione di tale luogo resterebbe comunque non univoca.

E allora il percorso da seguire per favorire la formazione di professionalità di alto livello, sia nella magistratura che della polizia giudiziaria, non può che essere – a mio avviso – quello di stabilire, per legge, la competenza territoriale nella materia della criminalità informatica, privilegiando la concentrazione delle indagini su pochi e più performanti uffici.

4. La transnazionalità e la mutua assistenza internazionale

Da parte di chi mi ha preceduto, si è fatto cenno, assai autorevolmente, anche alla "transnazionalità" come costante caratteristica della criminalità *cyber*.

Intendo riprendere, anch'io, l'argomento ma solo per sottolineare l'importanza del recente Protocollo Addizionale alla Convenzione di Budapest sulla criminalità informatica, il cui scopo essenziale è favorire una "*cooperazione rafforzata*" tra gli stati in relazione ad alcuni importanti scenari investigativi, che richiedono strumenti operativi sempre più efficaci.

La Ministra Cartabia, nel firmare il Protocollo (a Strasburgo il 12 maggio scorso), ha tra l'altro precisato: "*Questo costituisce una protezione preventiva per le vittime dei cyber crimini*" (…) "*le procedure di emergenza previste da questo trattato – che obbligano tutti i Paesi che ratificano il testo a creare canali specifici per una cooperazione rapida in situazioni in cui la vita o l'incolumità di una persona corrano un rischio imminente e grave – faciliteranno la prevenzione dei crimini più gravi*".

---

limiti della non arbitrarietà e della ragionevolezza, appartengono alla discrezionalità legislativa; mentre altre esigenze, quali quelle di agevolare la raccolta delle prove, di ridurre i disagi per le parti e per i testi, di assicurare un effettivo controllo sociale, di riaffermare la giustizia nel luogo in cui è stata violata, ben possono cedere dinanzi a valori costituzionalmente garantiti o a esigenze di pari, se non maggiore, rilevanza». Pertanto, «la nozione di giudice naturale non si cristallizza nella determinazione di una competenza generale, ma è frutto del complesso della disciplina attributiva della competenza, formandosi per effetto di tutte le disposizioni di legge, comprese quelle derogatorie alle regole ordinarie in base a criteri che ragionevolmente valutino i valori in gioco, anche di rango costituzionale, e i disparati interessi coinvolti nel processo».

Va ricordato che la Convenzione di Budapest del 2001 ha offerto la prima reale risposta globale nel contrasto alla criminalità informatica, alle frodi informatiche alla diffusione di materiale pedopornografico. Il Protocollo Addizionale del 2022, preso atto della complessità degli scenari e della gravità delle conseguenze dei *cyber* crimini, semplifica al massimo la mutua assistenza tra gli Stati Parte.

Il nuovo strumento giuridico, adottato da 22 Paesi, facilita e velocizza l'accesso delle Autorità giudiziarie e delle polizie alle prove elettroniche detenute dagli *internet provider*.

Fondamentale è la definizione del concetto di «emergenza» come *una situazione in cui vi sia rischio considerevole o imminente per la vita o la sicurezza di una persona fisica*, ricorrendo la quale è possibile per ciascuno degli stati aderenti al protocollo fare affidamento su un punto di contatto reperibile 24 ore su 24 cui trasmettere una richiesta di assistenza immediata. Sono indicati anche i contenuti minimi di tale richiesta, che esula dagli ordinari strumenti di natura rogatoriale; si tratta, piuttosto, di un meccanismo flessibile che potrà consistere in una semplice *mail* ovviamente trasmessa e ricevuta con adeguati livelli di sicurezza e autenticazione.

È anche precisato, nel Protocollo, che le richieste possono essere inviate alle Autorità giudiziarie direttamente oppure attraverso i canali dell'Interpol o facendo riferimento al punto di contatto (disponibile 24 ore su 24) istituito in conformità alla Convenzione.

È prevista la videoconferenza quale ulteriore strumento idoneo allo scambio di informazioni, sempre nell'ottica di garantire la più efficace e tempestiva assistenza giudiziaria tra le Autorità procedenti degli Stati Parte.

E facendo uno sforzo di fantasia si può immaginare, in prospettiva, un'organizzazione ancora più strutturata, magari prendendo a modello quanto è stato fatto per l'istituzione dell'EPPO.

5. Alcune note conclusive

Non posso terminare questo breve intervento senza fare almeno un cenno all'Agenzia per la Cybersicurezza Nazionale (ACN).

Con il decreto-legge 14 giugno 2021, n. 82 è stata ridefinita l'architettura nazionale *cyber* e istituita l'Agenzia per la Cybersicurezza a tutela degli interessi nazionali nel campo della "cybersicurezza".

All'Agenzia è anche riservato il compito di assicurare il coordinamento tra i soggetti pubblici coinvolti nella materia e, in particolare, di promuovere

azioni comuni mirate a garantire la sicurezza cibernetica.

È stato immediatamente notato che il citato decreto non prevede una cooperazione interistituzionale con la magistratura. Tale mancanza è per certi versi criticabile, posto che ogni attacco informatico è anche un reato, che prevede il necessario e obbligatorio intervento del magistrato.

Ma a prescindere dall'iscrizione del procedimento penale e dalle previsioni normative, il raccordo è comunque auspicabile; si pensi agli "atti pretipici" rispetto ad un attacco *cyber* (per esempio la predisposizione da parte dell'attaccante delle "risorse informatiche"): tecnicamente essi sono fatti non costituenti reato; è però innegabile che la condivisione del dato può favorire la soluzione di casi già al vaglio del pubblico ministero in cui l'attacco portato a termine presenti analogie con altri atti pretipici.

Dall'esempio proposto si coglie l'eccezionale rilevanza del coordinamento in questa delicata materia – che sicuramente si raggiungerà – tra l'Agenzia e la Magistratura.

Ma il coordinamento deve essere accentuato anche all'interno della magistratura.

Porto alla vostra attenzione – e così mi avvio alla conclusione – il seguente ragionamento.

Dietro un attacco *cyber* ci può essere uno Stato – c.d. attacco ibrido – o la criminalità organizzata, posto che il "ragazzino" che viola i sistemi di sicurezza del Pentagono per dimostrare a sé stesso, prima che agli altri, la propria bravura non è (più) "storia" che rientra nella realtà.

Alla criminalità organizzata, se non ha le risorse *in house* per compiere l'attacco finalizzato all'estorsione, non mancano di certo i mezzi per agire ricorrendo all'*outsourcing*.

Può capitare che – per fare un esempio – a Milano si indaghi su un attacco *cyber* che si sospetta essere opera di una cosca dedita, tra l'altro, anche alle "*cyber* estorsioni", cosca – nel nostro esempio – indagata anche dalla DDA di Palermo. L'indagine della Procura di Milano, riguardando un reato distrettuale ma che non rientra nella competenza della direzione distrettuale del capoluogo lombardo, solo per una fortuita e fortunata combinazione potrà beneficiare di utili informazioni magari in possesso della Procura distrettuale di Palermo.

Eppure il coordinamento, in casi del genere, sarebbe necessario.

Forse, la Procura Nazionale Antimafia potrebbe svolgere questo compito di raccordo, ma perché ciò sia possibile occorre l'intervento del Legislatore.

La definizione di *cyberspace*/spazio virtuale: approcci diversi alla regolazione

di Laura Carpini*

Con questo intervento cercherò di portarvi nella dimensione esterna, fattaprincipalmente di rapporti tra Stati, per cercare di comprendere meglio lo stato attuale del dibattito internazionale sulla definizione e sulla regolamentazione diuno spazio nuovo che, per tanti versi, sfugge ai parametri, alle norme dicomportamento e al diritto internazionale che si è andato cristallizzando nei secoli.

Dobbiamo quindi lasciare la dimensione interna dove lo Stato agisce con piena titolarità di sovranità e di poteri di ordine pubblico, per raggiungere un'area dove ogni Stato è uguale – sovranamente uguale – all'altro, dove vigonole regole del diritto internazionale, con le caratteristiche che gli sono proprie.

Il primo dato che vorrei portare alla vostra attenzione è che a livello internazionale non esiste una definizione di cyberspazio su cui tutti gli Stati delleNazioni Unite abbiano concordato. Esiste piuttosto una prassi di utilizzo di questa espressione, che peraltro è stata coniata in un romanzo di fantascienza diqualche decennio fa. Questo elemento è già sufficiente per intuire le difficoltà che gli Stati sperimentano nel relazionarsi in questo nuovo spazio utilizzando parametri più tradizionali. Perché?

Il cyberspazio è un ambiente molto complesso, costituito da vari segmenti,che sfugge alla territorializzazione tradizionale che è elemento costitutivo della sovranità e dunque aspetto primario del diritto che regola poi i rapporti fra Stati.

In Italia abbiamo dato una definizione dello spazio cibernetico, che è contenuta nel d.P.C.M. Gentiloni del 17 febbraio del 2017, dove lo spazio cibernetico è definito come "*l'insieme delle infrastrutture informatiche interconnesse comprensivo di hardware, software, dati ed utenti, nonché delle relazioni logiche comunque stabilite fra di essi*"[1]. Con il più recente decreto-legge n. 82 del 2021, poi è stata introdotta una nuova definizione di cybersicurezza (art. 1), la quale viene intesa come "l'insieme delle attivitànecessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi

(*) Responsabile Unità per le politiche e la sicurezza dello spazio cibernetico, Ministero degli Affari Esteri e della Cooperazione Internazionale.

1) DPCM 17 febbraio 2017, *Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali* (17A02655) (G.U. Serie Generale n. 87 del 13-04-2017).

informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico"[2]. Si tratta quindi di definizioni molto ampie, che comprendono anche le relazioni che si possono svolgere all'interno dello stesso Paese, ma anche quelle tra gli utenti di Paesi diversi.

Ulteriore elemento di complessità è che il cyberspazio è diverso da Internet e dal World Wide Web.

Internet, nato nel 1970, è una realizzazione unica nella storia dell'umanità. È infatti un'infrastruttura aperta, distribuita e governata da una comunità multilaterale e multi-stakeholder, dove per multi-stakeholder si intende una comunità composta sì da attori governativi, ma anche dagli attori privati che creano, mantengono e innovano le reti.

Poi c'è il web, inventato negli anni '90 in Europa, che è il luogo dove si svolgono estensivamente interazioni tra soggetti, anche privati, che condividonocontenuti e dati.

Esistono ulteriori elementi di complessità come i social network, i quali però – nonostante detengano una profonda importanza e influenza dal punto divista dei contenuti, di aspetti sociali e del rispetto dei diritti degli utenti, solo percitarne alcuni – non saranno discussi approfonditamente in questa sede.

Ecco quindi che gli Stati nazionali – gli attori principali delle relazioni internazionali analogiche – nel cyberspazio sembrano perdere forza rispetto alle grandi ditte o agli enti non governativi che gestiscono infrastrutture transnazionali per definizione, e che sempre di più assumono il ruolo di attori dell'evoluzione e dell'innovazione. Certo, il primo messaggio di posta elettronica della storia fu lanciato nel 1969 su ARPANET (una infrastruttura appartenente alla rete del Pentagono che può essere considerata l'antenata di Internet) ma il vero sviluppo si è avuto attraverso le reti universitarie, e successivamente grazie alle cosiddette "Big Tech". Inoltre, quanto precede rappresenta solo una fase di un processo in rapida e continua evoluzione; a breve avremo un "Internet-of-Things" pervasivo, stiamo assistendo alla nascita di vere e proprie "Smart Cities", ed assisteremo all'avvento del "quantum computing", il quale accrescerà esponenzialmente il livello di connessione, l'impatto sulle nostre vite e, almeno in Occidente, il ruolo degli attori privati nel sistema.

Un esempio su tutti è ICANN – l'Internet Cooperation Assigned Names and Numbers – che gestisce l'operato dell'Assigned Numbers Authority (IANA), la quale a sua volta coordina e gestisce il Domain Names System (DNS), il sistema preposto alla gestione di internet, fondamentale per l'ac-

cessibilità dei siti web e per l'instradamento della posta elettronica. ICANN è stata fondata nel 1998 per decisione del governo degli Stati Uniti di cedere la gestione politica e tecnica del DNS ad un ente privato no-profit a partecipazione globale.

I Governi dei vari Paesi partecipano ad ICANN solo a titolo consultivo in un comitato che si chiama GAC – Government Advisory Committee – e la gestione operativa della rete è affidata a questo ente no-profit.

A fronte di questo grande sviluppo tecnologico caratterizzato da una gestione multi-stakeholder – quindi non esclusivamente composto da attori statali – i regimi autoritari percepiscono Internet e le sue caratteristiche come un potenziale pericolo per la propria sovranità ed indipendenza. Da diversi anni questi Paesi stanno cercando di aumentare la propria indipendenza dalla rete globale e isolare il traffico nazionale esercitando un forte controllo sui contenuti. Più in generale, negli ultimi 25 anni alcuni Paesi hanno realizzato diversi tentativi di cambiare la struttura e il funzionamento di Internet, per ricondurli nella dimensione puramente intergovernativa e sovrana. Lo hanno fatto principalmente attraverso iniziative tecnico-diplomatiche in ambito multilaterale, ma anche dotandosi a livello interno di numerosi strumenti normativi a supporto di una forte prevalenza dello Stato su tutto ciò che riguarda le reti e l'uso dei dati. Tanto che, sempre di più, nel dibattito internazionale si parla di un possibile "Splinternet", cioè di una frammentazione di Internet.

Quanto precede è di estrema rilevanza anche per chi ha responsabilità di protezione dell'ordine pubblico e di amministrazione della giustizia, perché la capacità di essere più efficaci nelle indagini e nel perseguimento dei reati deve nutrirsi di una forte collaborazione internazionale. Nel cyberspazio tutto si svolge con una tale rapidità e pervasività che questo tipo di collaborazione necessita di un alto livello di fiducia e di integrazione tra Paesi. Fiducia reciproca, consuetudine di rapporti di collaborazione giudiziaria, disponibilità alla condivisione di dati e informazioni che attengono alle funzioni più caratterizzanti e interne dello Stato, condizioni che risultano estremamente difficili da ottenere in un ambiente internazionale caratterizzato da visioni e interessi diametralmente opposti, sfiducia crescente e tendenza alla frammentazione tecnica.

In questo contesto, l'Unione Europea sta cercando di rispondere alla sfida attraverso la forza del proprio potere regolatorio e persegue una propria autonomia per stimolare l'innovazione interna e proteggere i diritti dei propri

cittadini senza lederne le libertà e le opportunità offerte dalla rete globale. Uno degli esempi di maggior successo è il regolamento generale per la protezione dei dati personali dell'UE (GDPR), nato per proteggere i dati personali dei cittadini europei imponendo alcuni obblighi anche a soggetti esterni. Effetti simili si verificheranno attraverso l'applicazione della direttiva NIS2, attraverso la quale vengono definiti strumenti di tutela maggiori per la nostra sicurezza. A titolo esemplificativo, menzionerei inoltre i progetti di Cloud europeo e nazionale, in quanto dispositivi che potrebbero aiutare l'Unione Europea ad ottenere una maggiore disponibilità e protezione dei propri dati, e pertanto favorire tutte le attività di giurisdizione ad esse connesse.

La relazione con il settore privato può dunque essere assai sfidante anche per i Paesi europei, le cui visioni ed interessi possono non coincidere con quelli di alcune imprese. Immaginiamo quanto forti possano essere gli interessi delle grandi "Big Tech" americane rispetto a un mercato europeo che vuole essere sempre più autonomo e diversamente regolato rispetto a quanto avviene negli USA.

Le questioni sono dunque molto complesse, spesso più di quanto appaia, anche tra Paesi ed organizzazioni internazionali che in qualche modo condividono gli stessi valori. Dato questo quadro, a livello di collaborazione internazionale non abbiamo ancora raggiunto un livello adeguato soprattutto considerando l'importanza di avere regole condivise nella materia, vista la pervasività ed il sempre maggiore ricorso a strumenti digitali in tutti gli aspetti della nostra vita. A livello ONU si sono però ottenuti due grandi processi.

Il primo consiste nel Gruppo di Esperti Governativi (GGE), che si è riunito diverse volte dal 2004 in avanti, il cui principale risultato è stato il rapporto del 2015 dove è stata affermata l'applicabilità del diritto internazionale allo spazio cibernetico. Nonostante possa sembrare una banalità, questa è invece una grande conquista perché sancisce la legittimità di poter adottare, ad esempio, la Carta delle Nazioni Unite ed i principi in essa contenuti come base per regolare i rapporti tra Stati in questo ambiente. Il GGE ha facilitato inoltre l'adozione di 11 norme di comportamento responsabile, che sono tuttavia non vincolanti, poiché siamo nel campo della *soft law*. Esse tuttavia rappresentano un inizio di condivisione di comportamenti, che può cominciare ad essere percepito come vincolante dagli Stati, al fine di dare inizio a quel processo che poi porta alla formazione delle norme di diritto internazionale consuetudinario.

Il secondo grande processo a firma ONU consiste nella Convenzione di Budapest, secondo protocollo, che è stato firmato di recente dal Ministro della Giustizia. Al contempo, è stato avviato un negoziato per una nuova convenzione globale sulla criminalità cibernetica.

In riferimento a questo processo, l'Italia ha fatto la propria parte, cercando di contribuire allo sforzo degli altri Paesi per cristallizzare una forma di diritto internazionale. Come noto, a novembre 2021 è stata pubblicata una posizione internazionale sull'applicabilità del diritto internazionale allo spazio cibernetico dove abbiamo ribadito la regola della sovranità ma anche la *due-diligence*, cioè l'obbligo degli Stati di non permettere che il proprio territorio venga usato per azioni malevole, nel rispetto per i diritti umani ed in considerazione della cooperazione internazionale.

In conclusione, tenevo a condividere questo messaggio: in un ambiente caratterizzato da forte instabilità e scarsa regolamentazione condivisa, due visioni contrapposte si fronteggiano. All'interno di quella occidentale a sua volta si manifesta la presenza di una sorta di *trade-off* tra la difesa di internet così multilaterale e diffuso – che non è interamente gestito dagli Stati – e dall'altra parte le esigenze di sicurezza, tutela dell'ordine pubblico e amministrazione della giustizia, che necessitano di regolamentazione, dell'esercizio della giurisdizione e comportano l'affermazione della sovranità degli Stati. In questo *trade-off*, dove tireremo la linea, dove la tirerà l'Unione Europea? Il dibattito è aperto e non sempre è facile trovare risposte, vista la complessità della questione.

Nuove sfide dal cyberspazio: la questione dell'*attribution*

di Nunzia Ciardi*

Innanzitutto, permettetemi di ringraziare gli organizzatori di questa prestigiosa Conferenza per l'invito a prendervi parte. È per me sempre un gran piacere partecipare a dibattiti stimolanti e costruttivi, soprattutto su un tema che vede nella collaborazione e nello scambio tra istituzioni diverse e Paesi diversi la chiave di volta per la risoluzione di molti importanti problemi.

Lo sviluppo e la crescente pervasività di Internet e di nuove o emergenti tecnologie dell'informazione e della comunicazione hanno trasformato e continuano a trasformare profondamente la società contemporanea. Una significativa accelerazione sta caratterizzando la digitalizzazione di processi e contenuti, favorendo l'interconnessione tra gli individui e l'ambiente in cui questi vivono nonché ampliando significativamente i confini del cd. cyberspazio, nel cui ambito si svolgono, oramai, attività essenziali per il regolare svolgimento della vita individuale e collettiva.

Se, da un lato, il progresso tecnologico e lo sviluppo del cyberspazio contribuiscono a generare notevoli opportunità e benefici in termini di crescita economica, sociale, politica e culturale della collettività, dall'altro la espongono a nuove vulnerabilità, rischi e minacce, sempre più diffusi, diversificati e sofisticati. Condizione imprescindibile per far fronte a tali minacce è la disponibilità di opportuni strumenti – normativi, di policy e tecnologici – e capacità – istituzioni, risorse e competenze – da impiegare tanto a scopo preventivo quanto di risposta.

Tra le minacce cyber figurano quelle perpetrate da attori di natura non-statuale (individui o organizzazioni), per il perseguimento di finalità criminali. È il cd. fenomeno del cybercrime che, in termini generali, può essere definito come l'impiego di nuove o emergenti tecnologie e tecniche, associate al dominio cyber, per finalità delittuose. Si tratta di un fenomeno non nuovo e ben conosciuto, che consiste in una variegata serie di attività criminose che spaziano dalle frodi informatiche, all'accesso abusivo ad un sistema informatico, al drammatico fenomeno della pedopornografia on line, al terrorismo, al furto d'identità, fino all'organizzazione del gioco d'azzardo, di scommesse clandestine e di mercati illegali *on-line*.

Naturalmente, queste tipologie di attività criminali cyber non esauriscono

(*) Vice Direttore nazionale dell'Agenzia per la Cyber-Sicurezza Nazionale.

no la categoria del cybercrime, che è e un fenomeno articolato e in continua, rapida, evoluzione ed espansione, soprattutto per le capacità di attori criminali nuovi o tradizionali, più o meno organizzati, di operare in un "ambiente" in costante trasformazione, nonché di sfruttare abilmente le opportunità offerte dal processo di innovazione tecnologica. *Da questo punto di vista, il cybercrime continuerà ad evolvere e a trasformarsi di pari passo con il progresso tecnologico.* E l'espansione del fenomeno sarà tanto maggiore, continua e rapida quanto più il compimento di questi tipi di crimini si dimostrerà attrattivo per i singoli o i gruppi criminali, ovvero sarà "conveniente" in termini di rapporto costi-benefici. Da intendersi però non solo ed esclusivamente da un punto di vista economico.

Infatti, quello economico, sebbene sia il principale, non è l'unico incentivo a rendere il crimine informatico, in particolare, alcune sue fattispecie, attrattivo per gli individui o le organizzazioni che compiono queste attività. Alla possibilità di realizzare significativi proventi, bisogna aggiungere il percepito o, in molti casi, reale minor rischio che la condotta criminosa sia scoperta dalle autorità di *law enforcement* e che il responsabile venga incriminato.

Tale minor rischio è innanzitutto dovuto a diverse caratteristiche (tecniche e di funzionamento) proprie dell'ambiente cyber e delle tecnologie ad esso connesse, in particolare alla possibilità da queste garantite di assicurare, previa adozione di opportune soluzioni, l'anonimato degli utenti della rete. Come ben evidenziato nel rapporto pubblicato nel 2019 da Europol e Eurojust, relativo alle sfide al contrasto al cybercrime, la condizione di anonimato, garantito attraverso il ricorso a soluzioni crittografiche, determina la cd. "loss of location", che comporta la difficoltà di stabilire il "chi", il "come" e il "dove" di un'azione cyber criminale.

All'ostacolo rappresentato dall'anonimato si deve poi aggiungere la relativa inidoneità degli strumenti normativi, che dettano discipline preventive, a "tenere il passo" rispetto alle opportunità offerte dal progresso tecnologico ai criminali informatici. Si devono poi considerare i limiti degli strumenti operativi e delle procedure a cui possono ricorrere le autorità di *law enforcement* per l'esercizio di efficaci attività di indagine e di repressione.

A quest'ultimo riguardo, oltre alla difficoltà di reperire, formare e aggiornare competenze tecniche e specialistiche – tema di assoluta centralità – sussistono intrinseche difficoltà di svolgere efficacemente le attività di indagine e di contrasto, le quali, spesso, per la natura stessa del crimine in oggetto, assumono una connotazione transnazionale e presuppongono la collaborazione bi- o multilaterale transfrontaliera, non sempre agevole da attuare

concretamente. È evidente infatti che, quasi sempre, il raggio operativo del crimine informatico non si limita ad un solo Stato e a pochi individui sottoposti alla sua giurisdizione, ma può estendersi fino a ricomprendere molteplici giurisdizioni nazionali. *La rete ha sbriciolato ogni confine spazio-temporale.* Ordinariamente, è all'estero che si consuma, almeno parzialmente, la condotta criminosa e, tanto le tracce informatiche (sovente abilmente manipolate attraverso i più vari strumenti di anonimizzazione), quanto le tracce finanziarie (conti correnti e strumenti finanziari, sistemi di pagamento elettronico, corrieri di denaro, criptovalute, ecc.), frequentemente, riconducono fuori dal territorio nazionale. E dunque è naturale che l'attività investigativa soffra limitazioni e ostacoli originati dalla mancanza di uniformità delle legislazioni nazionali, che gli accordi internazionali in materia finora sembrano non riuscire a superare. Infatti, quello della criminalità cibernetica non è ancora un concetto giuridico definito, né compiutamente né in modo condiviso, comparendo – in relazione a specifici profili – in fonti sovranazionali ed europee.

Dunque, come dicevamo, *alta redditività e basso rischio* sono i principali elementi che sostengono l'espansione del crimine informatico; sono quelli che lo rendono fortemente attrattivo anche per il crimine organizzato "tradizionale", il quale, a tendere, potrebbe connotarsi sempre più come "cyber-mafia" o, comunque, servirsi di o generare sodalizi con esperti criminali informatici.

Infatti, così come hanno dimostrato di saper approfittare delle opportunità di arricchimento offerte dalla globalizzazione, le organizzazioni criminali di tipo mafioso sembrano interessate e intenzionate ad acquisire, direttamente o indirettamente, le capacità tecniche e le competenze che consentono loro di condurre attività criminose nell'ambiente cyber o per il suo tramite. L'acquisizione indiretta di capacità e competenze avviene attraverso il ricorso a professionisti singoli o ad altre organizzazioni criminali, che hanno sviluppato elevati gradi di specializzazione ed offrono *know-how*, *tool* e servizi sempre più complessi e raffinati, "pronti all'uso", secondo un modello che viene definito "crime-as-a-service". Da questo punto di vista, *le competenze informatiche diventano sempre più uno degli asset appetibili per le holding criminali.*

Anche se spesso sembra che le grandi mafie transnazionali non abbiano ancora investito in maniera massiccia, strutturata e uniforme nel crimine informatico, secondo diversi osservatori, negli ultimi anni, soprattutto in concomitanza con la pandemia, si è riscontrata una certa contiguità tra organizzazioni criminali "tradizionali" e realtà cybercriminali. Si starebbero cioè definendo le condizioni affinché il rapporto tra i due mondi criminali diventi

maggiormente consolidato.

Un ambito nel quale tale sodalizio è più evidente o potrebbe presto addirittura configurarsi come inquadramento organico è quello del cd. cybercrime finanziario. Questa tipologia di reati, infatti, pone il vantaggio per la criminalità di fornire un immediato riscontro economico alle attività delittuose. Grazie all'utilizzo di criptovalute, il brokeraggio, le frodi e le transazioni finanziarie occulte potrebbero diventare una significativa area di business per il crimine organizzato. Ma non solo. In realtà, vi sono diverse evidenze investigative che dimostrano come alcune mafie già da tempo utilizzano le monete virtuali per il pagamento di partite di stupefacenti. Come recentemente affermato dalla Direzione Investigativa Antimafia italiana ormai sono anni che alcune organizzazioni criminali utilizzano questo agile strumento per trasferire in Sudamerica le somme di denaro con cui pagare narcotrafficanti e produttori di droga colombiani.

A prescindere dalla specifica condotta illecita, *le transazioni di criptovaluta* legate all'attività criminale hanno raggiunto un nuovo record nel 2021 e *sono quasi raddoppiate* rispetto all'anno precedente, anche se la loro quota si sta riducendo in un mercato in forte espansione. Secondo uno studio della società Chainalysis sull'utilizzo della moneta virtuale, nel 2021 sono transitati attraverso conti legati ad attività illegali l'equivalente di 14 miliardi di dollari, una cifra quasi doppia rispetto ai 7,8 miliardi nel 2020. Secondo lo stesso studio, le transazioni illegali rappresentano però solo lo 0,15% dell'utilizzo totale delle criptovalute che lo scorso anno hanno movimentato transazioni per 15,8 trilioni.

Tuttavia, qualora si compisse quella saldatura definitiva tra crimine informatico e organizzazioni mafiose, che dispongono di gigantesche risorse di capitali, la percentuale delle transazioni illegali sul totale dell'utilizzo delle valute virtuali sarebbe destinato a crescere, così come il suo impatto sull'economia legale e sulla società nel suo complesso.

Guardando, appunto, ai profili appena delineati dal punto di vista delle autorità di *law enforcement*, tanto l'anonimato garantito dalla rete e da nuove soluzioni tecnologiche, quanto la transnazionalità del crimine informatico, rappresentano gli elementi che rendono difficoltosa la cd. *attribution*, tecnica e/o operativa, di un'azione criminale condotta tramite, nel o a danno del cyberspazio. Ostacolano, in ultima analisi, il processo che permette di individuare l'esecutore o il responsabile di un'azione criminale.

In quanto processo, l'attribuzione può essere definita come una serie di operazioni fattuali (*e.g.* raccolta di informazioni) o di ragionamento svolte in modo strutturato e logico al fine di ascrivere o imputare, con il fatto e con

giudizio, un'azione malevola cyber ad un'agente[1]. Più semplicemente, l'attribuzione è quel procedimento attraverso il quale si cerca di rispondere a due fondamentali domande: "Chi è stato (agente o esecutore materiale) a compiere una determinata azione?"; "Chi è il responsabile (soggetto suscettibile di giudizio) di quell'azione?". Domande le cui risposte vengono formulate sulla base di differenti, seppur strettamente interrelati, piani d'indagine.

La determinazione del "che cosa", del "come", del "dove" e del "chi" è dunque ostacolata dall'utilizzo da parte dei soggetti criminali di soluzioni di crittografia o altri simili espedienti, che garantiscono loro l'anonimato o "l'invisibilità", ovvero è ostacolata dalla transnazionalità della condotta criminosa che rende difficoltosa la definizione della competenza e della giurisdizione e limita le indagini, in particolare, la raccolta dell'*evidence*.

Ancora una volta, non può non rilevarsi come la "de-territorializzazione" dei fenomeni di cyber-crime si scontri con una giurisdizione tradizionalmente legata al territorio. Da questo punto di vista, un risultato normativo di segno chiaramente positivo si è conseguito con l'istituzione della Procura europea (EPPO[2]). L'intuizione della costruzione quale ufficio unico a struttura decentralizzata, e la previsione di poteri esecutivi diretti, mirano ad attuare una concreta cooperazione rafforzata che, nei reati economici-finanziari che la Procura europea persegue, rende superate una serie di strumenti tradizionali. La Procura europea sembra, pertanto, poter essere una intelligente e fruttuosa risposta all'esigenza di superamento dei confini territoriali, almeno nell'ambito dell'Unione.

Pensiamo a esempio al *cyberlaundering* che rappresenta una manifestazione parziale dell'ampio fenomeno del cybercrime[3]. Come osservato dalla dottrina penalistica, il *cyberlaundering* appartiene alla categoria dei reati

1) M.E. Bonfanti, *L'attribuzione di operazioni cibernetiche quale requisito e strumento di risposta*, in U. Gori, *Information Warfare 2018. Dalla Difesa Passiva alla Risposta Attiva*, Milano, 2019, pp. 32-46.

2) La Procura europea (EPPO), istituita dal regolamento (UE) 2017/1939, del 12 ottobre 2017, relativo all'attuazione di una cooperazione rafforzata sull'istituzione della Procura europea, è un organismo indipendente dell'Unione europea che indaga, persegue e porta in giudizio i reati che ledono gli interessi finanziari dell'UE (quali frodi, corruzione, riciclaggio, frodi IVA transfrontaliere). L'EPPO è diventata operativa il 1° giugno 2021 e vede l'adesione di 22 Stati membri rispetto ai quali ha poteri diretti. L'EPPO ha una struttura a due livelli. Un livello centrale con sede a Lussemburgo e costituito da un Procuratore Capo europeo e un collegio dei procuratori che definiscono gli obiettivi strategici dell'organo. Un livello nazionale costituito dai procuratori europei delegati e dalle camere permanenti. I procuratori europei delegati nei 22 Paesi dell'UE partecipanti sono responsabili dello svolgimento di indagini penali e dell'azione penale e operano in piena indipendenza dalle rispettive autorità nazionali, mentre le camere permanenti monitorano e indirizzano le indagini e adottano decisioni operative.

3) Sul tema si veda estensivamente, nel testo e nelle note, M. Croce, *Cyberlaundering e valute virtuali. La lotta al riciclaggio nell'era della distributed economy, in Sistema penale*, 4/2021, pp. 127 ss.

informatici in senso lato, ovvero alle condotte criminose, nella specie il riciclaggio, compiute avvalendosi di uno strumento informatico come mezzo e non come oggetto materiale del reato.

Se le prime manifestazioni criminose rivolte allo sfruttamento delle nuove tecnologie a fini di riciclaggio risalgono a diversi anni orsono, è stato solo con l'avvento delle valute virtuali che il fenomeno ha avuto una crescita esponenziale, in quanto le operazioni con tali strumenti permettono il consolidamento dei proventi delittuosi, *senza alcun previo passaggio per la dimensione reale dell'economia.* È possibile dunque affermare che il *cyberlaundering* compiuto servendosi delle valute virtuali rappresenta oggi la nuova frontiera del riciclaggio. Secondo il già citato studio di Chainalysis, nel 2021, attraverso il ricorso alle valute virtuali, si stima che sia stato riciclato l'equivalente di 8.6 miliardi di dollari, il 30% in più rispetto alle somme di danaro che sarebbero state riciclate, sempre tramite criptovalute, nel 2020. In totale, a partire dal 2017, si stima che sia di 33 miliardi di dollari il valore delle somme riciclate.

Ma cosa sono esattamente le valute virtuali o le criptovalute? In termini generali, si tratta di valute che non esistono in forma fisica (anche per questo viene definita "virtuale"), ma che si generano e si scambiano esclusivamente per via telematica[4]. Tra le principali criptovalute utilizzate dagli utenti di Internet figurano Bitcoin, Ripple, Ethereum, Solana, per citarne alcune. Le criptovalute hanno caratteristiche peculiari; il loro funzionamento si basa su: (i) un insieme di regole (detto "protocollo"), iscritte in un codice informatico che specifica il modo in cui i partecipanti possono effettuare le transazioni; (ii) una sorta di "libro mastro" (*distributed ledger* o *blockchain*), che conserva immodificabilmente la storia della transazioni; (iii) una rete decentralizzata di partecipanti che aggiornano, conservano e consultano la *blockchain* delle transazioni, secondo le regole del protocollo. Una volta emesse, le valute virtuali possono essere acquistate o vendute su una piattaforma di scambio (cd. *exchange platform*), utilizzando denaro a corso legale (per esempio, EUR, USD, ecc.). Le piattaforme di scambio su cui si acquistano e vendono valute digitali non sono attualmente regolamentate.

A rendere particolarmente attraente la valuta virtuale agli occhi degli investitori è la perfetta fusione dei vantaggi della moneta reale e di quelli della moneta elettronica in essa riscontrabile[5]. Come la moneta fisica, quella virtuale è accessibile a chiunque, ha carattere anonimo ed è agevolmente trasferibile; come la moneta elettronica, consente di effettuare agevolmen-

4) Si veda *https://www.consob.it/web/investor-education/criptovalute.*
5) M. Croce, cit., p. 129 ss.

te pagamenti a distanza e garantisce transazioni rapide e a basso costo. Le transazioni in valuta virtuale sono un formidabile veicolo di business, poiché consentono agli operatori economici di entrare in contatto con le più svariate realtà internazionali e di interagire con le stesse a costi ridotti e con possibilità di perfezionare in modo istantaneo trasferimenti di ingenti somme di denaro. Di recente, la preoccupazione sulla forza attrattiva del mercato delle criptovalute è particolarmente sentita anche a seguito del conflitto Russia-Ucraina, per il timore che si possano utilizzare le criptovalute per aggirare le severe sanzioni economiche adottate contro la Russia.

Per le ragioni appena esposte, le valute virtuali hanno attirato su di loro l'attenzione dei criminali informatici e delle cyber-mafie. In particolare, l'anonimato o lo pseudo-anonimato garantito agli utenti di valute virtuali è il principale elemento che induce la criminalità a sfruttare la piazza finanziaria digitale *per polverizzare le ingenti liquidità di origine illecita*[6]. Infatti, le infrastrutture basate sulla tecnologia *blockchain*, sebbene permettano a chiunque di visionare le transazioni effettuate dagli altri nodi della rete, verificandone l'importo e individuando gli indirizzi dell'ordinante e del beneficiario, non consentono, tuttavia, di risalire all'identità dei singoli utenti. Sul pubblico registro le transazioni sono infatti catalogate in stringhe numeriche esadecimali corrispondenti agli indirizzi di invio/recezione della valuta (*transaction address*). Peraltro, gran parte dei protocolli di gestione delle transazioni consente agli utenti di formare identificativi differenti per ogni singola transazione, rendendo difficoltosa, se non impossibile, l'identificazione dei titolari degli accounts coinvolti.

La criptomoneta, dunque, consente di inviare e ricevere denaro con garanzie di anonimità come nessun altro sistema al mondo. Non si può non notare che anche gli Stati storicamente più legati al segreto bancario ammettono oggi ampie deroghe e riserve in forza degli accordi internazionali di mutua collaborazione in materia penale e/o tributaria. Del resto, anche se il riciclaggio del denaro si realizzasse in Paesi che garantiscono appieno il segreto bancario o in Stati che non prevedono presidi antiriciclaggio, i criminali dovrebbero comunque trovare un espediente per rientrare in possesso dei capitali ripuliti senza compiere operazioni sospette. L'utilizzo del circolante virtuale risolve a monte il problema, poiché, quale che sia lo Stato di residenza del destinatario finale delle somme, non esistono segnali "spia" o indicatori della illiceità della transazione[7].

Inoltre, la rapidità degli scambi di moneta virtuale rappresenta un serio

6) *Ibid.*
7) *Ibid.*, p. 137.

ostacolo all'identificazione della provenienza delittuosa del denaro, mentre l'accettazione su larga scala della valuta assicura l'*integrazione* del profitto attraverso semplici operazioni di acquisto di beni o servizi o scambio in altri valori virtuali. *A differenza dell'infrastruttura bancaria tradizionale, un ecosistema decentralizzato riduce drasticamente i tempi di transazione e permette uno scambio peer to peer, senza passare per soggetti terzi gravati dagli obblighi antiriciclaggio*[8].

In breve, la ripulitura del denaro online attraverso le criptovalute presenta per i criminali numerosi vantaggi, tra cui: la possibilità di agire in qualsiasi momento e in modo anonimo, senza che sia necessario interfacciarsi *de visu* con persone fisiche; l'opportunità di assoldare direttamente sul web terzi fiduciari per il compimento delle operazioni intermedie (*money mules*); le difficoltà nell'individuazione del *locus commissi delicti* e dell'identità dei soggetti coinvolti nella filiera del riciclaggio. Poiché la maggior parte delle valute virtuali sono accettate come mezzo di pagamento da un crescente numero di operatori economici, il rientro nel circuito dell'economia lecita potrà realizzarsi anche senza la previa conversione in moneta avente corso legale, semplicemente acquistando beni o servizi. L'utilizzo delle valute virtuali massimizza i vantaggi, rendendo assai più agevole la movimentazione dei capitali[9].

Quanto descritto può dare il senso delle difficoltà che le autorità di *law enforncement* incontrano nel realizzare efficaci attività di prevenzione e contrasto ed evidenzia l'esasperazione delle principali sfide e dei limiti relativi alla lotta al cybercrime già accennati.

L'espansione del fenomeno dei cryptoasset sembra porre una sfida significativa alle autorità regolatorie, e cioè quella di governare l'innovazione operando un bilanciamento tra le esigenze stringenti di tutela e l'accesso a servizi adeguati. In questo senso, segnali decisamente positivi si possono rilevare nell'attività dell'Unione europea che sta acquisendo una vera e propria leadership, avendo optato per lo strumento legislativo del Regolamento, con l'obiettivo, appunto, di creare un quadro normativo di riferimento immediatamente applicabile in tutto il mercato unico. Ci si riferisce alla c.d. proposta MiCAR[10] (presentata dalla Commissione europea in data 24 settembre 2020 e attualmente in fase attiva di trilogo[11]) , con cui vengono definite una serie

8) *Ibid*.
9) *Ibid*.
10) COM/2020/593 final. Proposta di regolamento del Parlamento europeo e del Consiglio relativa ai mercati delle cripto-attività e che modifica la direttiva (UE) 2019/1937 ("Regolamento MiCA" o "MiCAR").
11) Negoziazione tra Commissione, Consiglio e Parlamento.

di regole applicabili alle offerte di cripto-attività non assimilabili a strumenti finanziari, depositi o depositi strutturati ai sensi della legislazione dell'UE in materia di servizi finanziari.

Altro fenomeno indicativo è l'estorsione condotta attraverso l'impiego di *ransomware* che rappresenta una tipologia di crimine informatico dilagante, insidioso e in progressiva evoluzione, che interessa non solo le infrastrutture informatiche di interi comparti economici/industriali, ma anche, in modo diffuso, quelle in uso a utenti individuali.

Stando a quanto evidenziato dai principali report sulla cybersecurity riferiti all'anno 2021[12], *il 35% delle intrusioni in sistemi informatici* integra il ricorso a ransomware. Si tratta di una tipologia di attacchi che, rispetto al 2020, mostra *una crescita* nell'ordine del *105%-107%.* In termini numerici non percentuali, la minaccia ransomware è complessivamente consistita in circa 623,3 milioni di azioni malevole, con significative conseguenze, non solo economiche, ma anche sociali, nella misura in cui ha determinato l'interruzione dell'erogazione di un servizio pubblico essenziale. Il riscatto medio pagato per recuperare i dati, che si attesta sui 812.360 dollari, è quintuplicato rispetto allo scorso anno e il 46% delle aziende i cui dati sono stati criptati a seguito dell'attacco ha deciso di pagare il riscatto. Nel nostro Paese il 55% delle aziende colpite ha dichiarato che l'impatto sulla propria operatività di business è stato molto alto e che il tempo di recupero dei dati è stato di "fino a una settimana" per il 36%, "fino a un mese" per il 34%, mentre solo l'11% del campione ha ripristinato la normalità in "meno di un giorno".

Ma che cosa è più esattamente il ransomware? Si fa, in particolare, riferimento ad una specifica tipologia di attività criminosa, recentemente salita agli onori della cronaca e che, oltre a profili strettamente penalistici, può sollevare questioni riguardanti anche la salvaguardia della sicurezza nazionale dello Stato. Si tratta dell'impiego dei cd. *ransomware*, ovvero di software malevoli *che cifrano i dati e li rendono indisponibili al loro legittimo titolare*, soggetto o organizzazione che sia. Per il "rilascio" di questi dati viene richiesto il pagamento di un riscatto in moneta virtuale. È una minaccia sempre più diffusa e che interessa un'ampia gamma di organizzazioni, private e pubbliche. I profili di sicurezza nazionale connessi alla minaccia emergono quando il *ransomware* colpisce e compromette sistemi informatici da cui dipende l'esercizio di una funzione essenziale o l'erogazione di un servizio essenziale dello Stato.

La condotta consumata attraverso il ransomware è caratterizzata da due

12) "*Navigating New Frontiers*" - Trend Micro 2021 Annual Cybersecurity Report, marzo 2022; *Microsoft Digital Defence Report*, ottobre 2021.

fasi: la prima, a scopo preparatorio, consistente in un'intrusione informatica seguita da una esfiltrazione dei dati; la seconda, integrante la minaccia telematica con richiesta di pagamento di riscatto. *L'esfiltrazione diviene strumentale al compimento dell'estorsione che, spesso, si configura come "doppia" o "tripla"*. I criminali, infatti, possono richiedere alla vittima il pagamento di una somma in criptovaluta per: (i) ottenere la chiave di decodifica dei dati, sbloccarne l'accesso e ripristinare il funzionamento del sistema (estorsione singola); (ii) scongiurare la pubblicazione di dati sensibili che potrebbe generare un danno d'immagine o di altro tipo; (iii) infine, evitare di subire un attacco DDoS (Distributed Denial of Service) contro eventuali servizi erogati dalla vittima.

L'organizzazione e il compimento di un'azione estorsiva che impiega il *ransomware* si può basare su strutture tanto centralizzate quando completamente decentralizzate. La parcellizzazione e decentralizzazione delle competenze e, soprattutto, delle azioni di cui sopra, spesso si associano alla distribuzione geografica, in diversi Paesi, dei loro esecutori e di chi ne è vittima.

Al riguardo si deve, però, rilevare che non sembrano esistere precedenti giurisprudenziali che condannino la vittima di un *ransomware* che abbia pagato il riscatto richiesto. Infatti, il reato di favoreggiamento sembrerebbe non potersi applicare in caso di persona fisica/privato, dal momento che, subendo la condotta, quest'ultimo verrebbe a configurarsi come mera vittima, soggetto passivo della commissione del reato, anche qualora decidesse di pagare il riscatto.

In alcuni Paesi è stato affrontato il tema di rendere illegale il pagamento del riscatto ma alla fine si è ritenuto che i problemi che sarebbero potuti derivare da una previsione del genere avrebbero superato gli eventuali vantaggi.

A diversa conclusione, invece, si potrebbe addivenire nel caso di pagamento del riscatto attraverso i soggetti terzi che si propongono alla vittima quali intermediari. In tal caso, potrebbe invero ben ipotizzarsi il reato di favoreggiamento, eventualmente introducendo, anche a chiari fini di manifestarne la contrarietà all'ordinamento giuridico, una specifica fattispecie di reato di favoreggiamento informatico.

Delineata brevemente la complessità del quadro – sia pure riferito a un numero ridotto di esempi – ci si chiede quali potrebbero essere le strade percorribili.

In linea di principio, occorrerebbe innanzitutto intervenire con riguardo all'utilizzo di soluzioni crittografiche che garantiscono l'anonimato e ostacolano l'*attribution*. Si tratta di una questione assai dibattuta, molto delicata e "spinosa", in quanto la crittografia o le altre soluzioni che assicurano l'anoni-

mato in rete (ad es. VPN, Tor) rappresentano, in determinate realtà, uno degli strumenti che tutelano gli individui/utenti dall'azione repressiva esercitata da regimi non democratici. Si pensi a regimi che tendono ad opprimere la libertà fondamentali degli individui di informazione ed espressione, anche *on-line*.

E anche se, come abbiamo detto, la crittografia può diventare un fattore abilitante per la commissione di crimini informatici non sembra praticabile – politicamente, giuridicamente, *ma neppure tecnicamente aggiungerei* – la via di limitare o vietare *tout court* l'utilizzo di soluzioni di crittografia, ovvero di indebolirne l'efficacia. Occorre necessariamente agire su altri piani.

La transnazionalità del cybercrime, risultante spesso dalla "parcellizzazione" funzionale e geografica delle azioni che integrano l'attività criminosa, *dovrebbe forse spingerci a una importante – quanto delicata – riflessione comune su alcuni aspetti della rete e delle società digitalizzate.* Una riflessione più allargata possibile. Che parta dagli elementi meno complessi e divisivi come l'importanza di norme applicabili a più giurisdizioni possibili (auspicabilmente di portata globale), in modo tale da evitare conflitti tra autorità di *law enforcement*, che possono ostacolare, ad esempio, la raccolta e circolazione del materiale probatorio. I fattori fondamentali per il successo di un'indagine sul cybercrime a dimensione internazionale sono infatti quello della velocità degli atti investigativi e della raccolta dei dati e di altra *evidence*. Dati la cui mancanza limita o impedisce la possibilità di eseguire correttamente *l'attribution*.

Nella consapevolezza di tali presupposti, la Convenzione di Budapest si ispira al massimo favore per la cooperazione internazionale. In questo senso, è di fondamentale importanza disporre di norme e procedure che favoriscano e sostengano l'efficace coordinamento e la cooperazione internazionale tra le autorità di *law enforcement*, limitando all'indispensabile le formalità burocratiche. Da un punto di vista pratico, il contrasto al crimine informatico è tanto più efficace quanto più è prevista e incentivata la possibilità di collaborazione transfrontaliera, da attuarsi anche attraverso la costituzione di *joint investigation teams*, e quanto maggiore è la propensione degli investigatori e degli inquirenti alla comunicazione e allo scambio informativo, alla rapida raccolta, conservazione e scambio dell'*evidence*, alla condivisione di esperienze, strumenti e professionalità tecniche. Propensione che va stimolata e coltivata costantemente, anche attraverso idonei programmi di formazione per gli operatori, *fino al punto in cui possa divenire una vera e propria mentalità o cultura professionale.* Come diversi casi della prassi dimostrano, l'efficace cooperazione internazionale diviene la chiave di volta per assicurare alla giustizia i responsabili della condotta criminale.

di Gian Luca Berruti*

1. Premessa: un nuovo approccio e una nuova metodologia investigativa grazie all'Intelligenza Artificiale

Come noto, la componente tecnologica ormai condiziona in maniera assoluta la quotidianità di una società in cui la capacità di far fronte ai ritmi frenetici che si è obbligati a sostenere, richiede un sempre più incisivo ricorso alla comunicazione digitale e alla necessità di essere costantemente connessi e presenti in rete.

L'utilizzo delle tecnologie permette di vivere un ambito senza confini, aldilà di qualsiasi barriera geografica, legislativa, sociale, creando un complesso reticolato di collegamenti che costituisce l'insieme delle infrastrutture del cosiddetto "mondo cibernetico".

Questo purtroppo vale anche per il crimine, sempre più spregiudicato nello sfruttare con immediatezza ed a proprio vantaggio qualunque innovazione disponibile sul mercato. Da qui l'escalation degli ultimi anni del crimine informatico, ormai sempre più centrale e propedeutico ad altre fattispecie di reato e in particolare al riciclaggio di denaro e altri beni come la criptovaluta.

Nel contrasto agli illeciti in rete, in piena sinergia con le altre forze di polizia e in particolare con la Polizia Postale e delle Comunicazioni, il Corpo della Guardia di Finanza esercita quindi un ruolo particolarmente importante a tutela delle libertà economico-finanziarie dei cittadini, delle istituzioni e delle imprese.

Lo esercita quotidianamente con la componente territoriale, dove spiccano apposite figure appositamente preparate, i CFDA[1] ma, per i casi di maggior complessità, lo svolge efficacemente con l'ausilio della componente speciale, una vera e propria élite di reparti, uomini e mezzi che ha competenza su tutto il territorio nazionale e spiccata proiezione internazionale. Tra questi il Nucleo Speciale Tutela Privacy e Frodi Tecnologiche è il reparto di avanguardia deputato alle investigazioni sulla rete ed al complesso ambito del contrasto al 'cybercrime', avvalendosi delle migliori risorse umane e delle ultime tecnologie in ambito informatico.

(*) Colonnello della Guardia di Finanza, titolato Corso Superiore di Polizia Tributaria, in servizio presso l'Agenzia per la Cybersicurezza Nazionale.

1) CFDA: Computer Forensics e Data Analyst.

Sul tema degli illeciti in rete, anche sulla base dell'esperienza operativa fin qui maturata, abbiamo quindi provato a considerare in concreto quali e quanti benefici l'intelligenza artificiale può apportare alla figura dell'investigatore dei nostri tempi e del futuro, una figura che immaginiamo a metà tra un analista e un operatore tradizionale. Abbiamo voluto farlo in concreto attraverso l'acquisizione e l'utilizzo per indagini di una piattaforma informatica dotata di un'interfaccia unica, semplice e di facile intuizione, in grado di unire e correlare tra loro, attraverso l'I.A., le cinque aree che riteniamo determinanti per poter svolgere efficacemente investigazioni 'native' in ambito digitale. Vediamole insieme.

2. La *Digital Forensics*

Alla base delle attività di indagine sono sempre più determinanti gli strumenti di digital forensics già disponibili sul mercato e muniti di intelligenza artificiale. Tra le tante definizioni, si può assumere quella secondo cui per digital forensics si intende: "*... l'uso di metodi scientificamente provati indirizzati a preservare, raccogliere, validare, identificare, interpretare, documentare prove digitali o comunque derivanti da sistemi digitali allo scopo di facilitare la ricostruzione di eventi di natura criminale già avvenuti o di aiutare a prevenire illeciti*"[2].

Molteplici e trasversali sono gli scenari operativi nei quali ricercare evidenze digitali ovvero, ad esempio: un sistema dal quale si esegue un accesso abusivo a un sistema informatico telematico; un sistema informatico oggetto di un accesso abusivo; files che contengono informazioni digitali; sistemi di comunicazioni; sistemi di pagamento per attività illecite utilizzati quali mezzi di attacco o quali vittime di reato.

Una volta individuato lo scenario operativo si procede al riconoscimento e all'acquisizione della fonte di prova digitale e soprattutto alla sua conservazione in modo da garantirne l'integrità. Gli strumenti informatici in dotazione alle forze di polizia in questo settore, prevalentemente di provenienza israeliana, sono già particolarmente evoluti e performanti e, sebbene in costante aggiornamento, necessitano solamente di essere messi 'a sistema' nella nostra piattaforma unica per garantire una celere e inappuntabile procedura propedeutica alla successiva indicizzazione del materiale ed alla consultazione.

2) Cfr. G. Costabile, *Digital Forensics & Digital Investigation: classificazione, tecniche e linee guida nazionali e internazionali*, G. Giappichelli, Torino, 2021.

3. La *Big Data Analysis*

L'analisi dei *Big Data*, ovvero la complessità delle analisi successive alla grande quantità di dati prodotta normalmente dalle acquisizioni forensi (ovvero da altre fonti di interesse probatorio), rende indispensabile avere a disposizione un apposito software anch'esso dotato di intelligenza artificiale nativa in grado di indicizzare e rendere correlabile in maniera snella ed efficace grandi quantità di informazioni.

Big data è infatti un termine applicato ai data set la cui dimensione o tipo supera la capacità dei database relazionali tradizionali di catturare, gestire ed elaborare i dati con bassa latenza. I big data possiedono una o più delle seguenti caratteristiche: elevato volume, elevata velocità o estrema varietà. L'AI[3], la tecnologia mobile, i social media e l'IoT[4] stanno portando la complessità dei dati verso nuove forme e fonti di dati. Ad esempio, i big data provengono da sensori, dispositivi, video/audio, reti, file di log, applicazioni transazionali, gran parte di essi viene generata in tempo reale e su vastissima scala. L'analisi dei big data mediante software di intelligenza artificiale consente ai nostri investigatori di prendere decisioni in modo più accurato e veloce, utilizzando dati precedentemente inaccessibili o inutilizzabili per avere subito un quadro chiaro degli elementi di possibile interesse investigativo con un importante razionalizzazione delle risorse umane deputate a questo scopo (pensate al tempo necessario a svolgere questa operazione manualmente!). Anche in questo campo sono diversi e performanti i prodotti offerti dal mercato: alla tecnologia nazionale si contrappone una vasta scelta di software a livello mondiale di cui beneficiano le nostre unità operative e che potremo agevolmente integrare nella nostra piattaforma e mettere a sistema.

4. Le *Cryptocurrency investigations*

All'interno di questa mole di dati potrebbero identificarsi delle tracce o dei 'semi' di cryptovaluta, la nuova frontiera delle transazioni digitali. Su questo argomento, come potete immaginare, la Guardia di Finanza è particolarmente attenta e sensibile sopratutto con riferimento al tema del riciclaggio e dell'aggressione patrimoniale. Man mano che il mondo delle cryptovalute[5]

3) AI: Artificial Intelligence - Intelligenza Artificiale.
4) IoT: Internet of Things.
5) *Criptovaluta*: una criptovaluta è una valuta virtuale che, secondo la definizione di Banca d'Italia, costituisce una rappresentazione digitale di valore ed è utilizzata come mezzo di scambio o detenuta a scopo di investimento. Le criptovalute possono essere trasferite, conservate o negoziate elettronicamente. Alcuni esempi tipici sono il Bitcoin, LiteCoin, Ripple, Ethereum, Cardano, Tron.

matura, queste assomiglieranno sempre di più alle valute legali che utilizziamo tutti i giorni; per ora, purtroppo, ci sono sicuramente dei rischi per coloro che si affacciano a questa nuova tecnologia restandone poi, truffati, tra cui purtroppo spesso gli attacchi di phishing[6], pratica che però riguarda qualunque tipo di servizio digitale ma che si è da subito adattata a questo nuovo sistema. Avviene tramite siti internet falsi che richiedono account personali, tramite mail o allegati contenenti virus o malware o ancora con profili fake sui social media e si rischia la perdita irreversibile della somma di denaro investita. C'è poi da precisare che le criptovalute, oltre ad essere strumento di "trasformazione o sostituzione" di beni o denaro, possono essere esse stesse proventi del reato. Pensiamo, ad esempio, agli illeciti tipici del mondo del cybercrime come Ransomware, truffe online o attacchi informatici che si avvalgono unicamente di questa tecnologia per tutti i pagamenti. Un mondo quindi nel quale ci imbatteremo sempre maggiormente e che ci deve trovare pronti e preparati ma sopratutto muniti degli strumenti informatici necessari.

5. Un approfondimento: le criptovalute, il riciclaggio e l'autoriciclaggio

Tornando al riciclaggio, occorre distinguere il "riciclaggio digitale strumentale" dal "riciclaggio digitale integrale": nel primo caso la cryptomoneta viene sfruttata solo per migliorare o favorire le tradizionali operazioni di 'laundering', che si svolgono secondo gli schemi delle operazioni classiche utilizzando i cryptoasset solo come un passaggio successivo (mediante un operazione di cambio del denaro) per sfruttarne la complessa tracciabilità e anonimizzazione e poi reimmettere le somme nel circuito dell'economia legale. Nel riciclaggio digitale integrale, tipico delle operazioni native in Crypto, tutte le fasi di riciclaggio avvengono mediante questi strumenti attraverso transazioni online che garantiscono lo pseudo-anonimato e impegnative difficoltà di controllo da parte delle autorità statali. Il riciclaggio digitale integrale è la forma di riciclaggio, dunque, ritenuta più pericolosa. Non vi è, infatti, alcun contatto materiale tra il riciclatore e il contante, ma l'operatore perfeziona il procedimento di laundering attraverso operazioni anonime e virtuali: è Il fenomeno del c.d. cyberlaundering. In questo contesto sono dunque indispensabili tracciamenti efficaci delle transazioni in criptovalute con correlazioni a entità del mondo reale e sopratutto un efficace presidio delle attività di Exchange e di cambio.

6) *Attacchi di phishing*: il *phishing* è un genere di truffa telematica che ha l'obiettivo di rubare le informazioni e i dati personali degli internauti.

Uno sviluppo positivo dell'ultimo anno è stato però la crescente capacità di alcune forze dell'ordine di diversi stati membri, tra cui la Guardia di Finanza per l'Italia, di riuscire a sequestrare i cryptoasset. Questo è molto importante non solo perché permette la restituzione delle somme alle vittime di crimini e allo stesso tempo la sottrazione delle stesse dagli scopi illeciti, ma anche perché smentisce la tesi secondo cui le criptovalute sarebbero non rintracciabili e non sequestrabili, ergo perfette per il crimine.

In virtù di quanto descritto è bene evidenziare che a gennaio 2022 è stato firmato dal Ministero dell'Economia il decreto che regola le attività degli operatori di criptovalute in ambito nazionale. In particolar modo il provvedimento disciplina l'iscrizione obbligatoria dei player in criptovalute nell'apposito registro che dovrà essere gestito dall'Organismo degli agenti e mediatori (Oam), tale iscrizione diventa prerequisito essenziale per esercitare legalmente l'attività. Un importante compito dell'Oam sarà proprio quello di collaborare con la Guardia di Finanza, la Direzione Antimafia nonché l'autorità giudiziaria e le agenzie fiscali fornendo periodicamente ogni informazione e documentazione necessaria, compresi i dati sulle operazioni effettuate.

Nell'ambito europeo, invece, la Commissione ha presentato una proposta di regolamento per la disciplina dei crypto-asset (c.d. MiCA). Tale pacchetto di riforme ha come obbiettivo quello di rendere il settore finanziario dell'Unione europea più competitivo, promuovendo un'innovazione responsabile con regole più sicure per i consumatori, e allo stesso tempo, più favorevoli allo sviluppo digitale. In questo ambito purtroppo la tecnologia nazionale è meno performante rispetto a quella straniera, americana in particolare; esistono però in commercio dei software dotati di I.A. in grado di riconoscere autonomamente tracce di cryptomoneta all'interno della nostra mole di dati indicizzata per la Big Data Analysis ed effettuare ogni possibile approfondimento su di essa. A nostro parere sono indispensabili.

6. Bot, Avatar e *Web Intelligence*

In questo nuovo scenario risulta complicato il continuo e assiduo controllo da parte del singolo investigatore ovvero la ricerca approfondita della rete di fatti e informazioni che, in maniera piuttosto intuitiva, possano portare ad esempio a identificare un criminale della rete. A questo potremo giungere se uniamo nella piattaforma dei moduli appositamente deputati alla Web-Intelligence, che consentono l'esplorazione efficace dei Social Media, purché

dotati di strumenti di ricerca per il Deep[7] e Dark Web[8] e consultabili nell'unica interfaccia intuitiva che ne consenta l'interazione automatica con i nostri software dedicati alle *Cryptocurrency Investigations* e alla *Big Data Analysis* permettendoci di effettuare in tempo reale correlazioni anche con eventuali evidenze digitali o elementi come chiavi pubbliche/private rinvenuti o oggetto di Leak.

La parte più interessante della nostra piattaforma informatica dotata di intelligenza artificiale riguarda però la possibilità di avvalersi della creazione, gestione e mantenimento di *BOT* e *Avatar* appositamente programmati di volta in volta per supportare le indagini e effettuare veri e propri pattugliamenti virtuali su tematiche-forum di interesse. A nostro avviso ottengono la massima efficacia quando si ricorre, nei casi in questo è consentito dalla legge, all'istituto dell'agente sotto copertura in rete. Al militare viene, di fatto, assegnata un'identità confacente ai fatti di indagine e opera in contatto e relazione con i cyber criminali o utilizzandone le piattaforme illegali presenti sul web e i nostri Bot lo supportano e rendono più credibile. Questo rimane lo strumento più efficace nel contrasto ai reati informatici: spesso le informazioni per de anonimizzare un criminale potrebbero essere già disponibili sulla rete e facilmente reperite per poi essere definitivamente acclarate mediante un'attività di polizia giudiziaria tradizionale (perquisizione, sequestro, ecc.).

7. Conclusioni

L'avvento delle criptovalute, il nuovo fenomeno degli NFT, il mondo virtuale più in generale, ha creato nuovi modelli criminali.

Sopratutto la diffusione delle nuove attività finanziarie legate alle cryptovalute e il loro apparente anonimato ha implicato che i criminali del web cominciassero da subito a utilizzare questi nuovi canali anche in maniera spregiudicata sfruttando talvolta anche la scarsa comprensione di un corretto utilizzo da parte degli investitori. Sicuramente gli interventi operativi delle forze di polizia denotano, ad esempio, un aumento dell'utilizzo della moneta virtuale nei mercati illegali (droghe, hacking, pedopornografia, omicidi), nel finanziamento al terrorismo, nel riciclaggio e nella sottrazione dei capitali alla tassazione. Possiamo quindi certamente testimoniare l'esistenza di una nuova

7) *Deep Web*: insieme delle risorse informative del world wide web non indicizzate dai normali motori di ricerca.
8) *Dark Web*: terminologia che si usa per definire i contenuti del World Wide Web nelle Darknet (reti oscure) che si raggiungono via internet attraverso specifici software, configurazioni ed accessi autorizzativi.

criminalità virtuale, per ora fortunatamente di nicchia, transnazionale spesso giovane e molto avvezza alle nuove tecnologie.

In questa direzione, oltre agli strumenti tecnologici, è sempre più determinante il ruolo della magistratura: all'efficace direzione di queste indagini va aggiunta l'importanza della cooperazione giudiziaria internazionale in questo settore, che è ormai divenuta imprescindibile.

La Guardia di Finanza si è fortemente evoluta e giocherà un ruolo sempre più determinante, insieme alle altre forze di polizia, nel campo del contrasto al crimine informatico le cui implicazioni sono praticamente sempre connesse all'illecito arricchimento ed al danno all'economia. In particolare, l'approccio del nostro investigatore economico-finanziario e delle risorse ormai tutte specializzate di cui disponiamo, dovranno sempre maggiormente abbinare, alla conoscenza delle tecniche di indagine tradizionale e della formazione orientata al '*follow the money*', le capacità tecniche proprie di un operatore specializzato in grado di acquisire, elaborare e processare le informazioni digitali proprio attraverso i nuovi strumenti informatici a disposizione.

In questo senso, come abbiamo sottolineato, un uso lungimirante dell'Intelligenza Artificiale come nel caso della piattaforma informatica 'olistica' e delle cinque aree di sviluppo che abbiamo analizzato, potrebbe consentire non solo di razionalizzare e valorizzare le risorse umane disponibili ma anche e sopratutto di fornire un contributo ed un efficacia determinante a tutte le investigazioni.

Bibliografia

Corte Suprema di Cassazione, sentenza nr. 02868 del 25.02.2022, in *www.gazzettaufficiale.it*

Costabile G., *Digital Forensics & Digital Investigation: classificazione, tecniche e linee guida nazionali e internazionali*, G. Giappichelli, Torino, 2021

Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della Guardia di Finanza, *Guida operativa in materia di investigazioni tecnologiche, digital forensics e data analysis*

Scuola di Polizia Economico-Finanziaria della Guardia di Finanza, *La sicurezza nelle nuove tecnologie*

www.borsaitaliana.it/borsa/glossario/criptovaluta

www.clusit.it/rapporto-clusit

www.cybersecurity360.it

www.ibm.com/it-it/analytics/hadoop/big-data-analytics

Dal *cybercrime* all'*artificial intelligence crime*. Brevi cenni sui profili penali

di Ivan Salvadori*

1. Introduzione

Verso la fine degli anni '70 del secolo scorso, i primi studiosi, in specie statunitensi, che si occuparono della criminalità informatica (*computer crime*), definirono gli emergenti fenomeni criminosi commessi mediante o a danno dei nuovi "oggetti" informatici (dati, *software* ed elaboratori) come *old wine in new bottles*. Secondo questo orientamento dottrinale, non vi era alcuna necessità, da parte dei legislatori nazionali, di introdurre norme incriminatrici *ad hoc*, dal momento che i comportamenti devianti facilitati dall'utilizzo abusivo degli strumenti informatici potevano essere pacificamente ricondotti nell'alveo dei reati tradizionali (furto, danneggiamento di cose, truffa, rivelazione di segreti d'ufficio, ecc.). A cambiare, in definitiva, sarebbero stati soltanto i mezzi o gli strumenti di esecuzione (*new bottles*) impiegati dai criminali, mentre il disvalore lesivo e, di conseguenza, la qualificazione giuridico-penale delle loro condotte sarebbero rimasti sostanzialmente invariati (*old wine*).

Ben presto, però, ci si rese conto, che assieme ad Internet erano nati anche nuovi "beni" informatici immateriali (dati e programmi informatici), non riconducibili al concetto tradizionale di «cosa», quale oggetto materiale di molti reati contro il patrimonio, ovvero di «documento», in relazione ai falsi documentali.

Pertanto, pur a fronte dei tentativi giurisprudenziali, spesso al limite del divieto di analogia *in malam partem*, di sussumere l'utilizzo abusivo degli strumenti informatici nelle fattispecie tradizionali, sempre più evidente fu l'oggettiva impossibilità di punire, in base alla legislazione penale allora vigente, i nuovi comportamenti criminosi (accessi abusivi a sistemi informatici, furto di *software*, *computer sabotage*, spionaggio di dati, ecc.). Per colmare le evidenti lacune normative, emerse nella prassi giurisprudenziale e sottolineate dalla dottrina più autorevole, molti legislatori nazionali, in linea con quanto previsto a livello sovranazionale, e in particolare dalla Raccomandazione R (89) 9 sulla "criminalità da elaboratore" del Consiglio d'Europa, introdussero nei loro ordinamenti giuridici norme incriminatrici *ad hoc* per contrastare il

(*) Professore associato di Diritto penale, Diirtto penale dell'ambiente e *International Criminal Law*, Dipartimento di Scienze Giuridiche, Università di Verona.

c.d. *computer-related crime*.

A livello europeo, l'Italia fu, dopo la Germania, tra i primi Paesi a comprendere la necessità di prevedere nuovi reati per contrastare le sempre più frequenti minacce connesse all'utilizzo abusivo delle tecnologie informatiche. Con la importante l. n. 547/1993, recante «*modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*», il nostro legislatore inserì nel codice penale un articolato quadro di reati informatici.

Nel 2008, il nostro Parlamento, seppur con notevole ritardo rispetto a quanto operato nella maggior parte dei Paesi europei, diede finalmente attuazione alle prescrizioni della Convenzione *cybercrime* del 2001 del Consiglio d'Europa. Con la l. n. 48/2008 vennero modificati alcuni reati informatici, introdotti nel codice penale nel 1993 (artt. 491-*bis*, 615-*quinquies*, 635-*bis* c.p.), e furono introdotte nuove fattispecie per punire la «*falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri*» (art. 495-*bis* c.p.), i danneggiamenti di dati e di sistemi informatici "pubblici" e "privati" (artt. 635-*ter*, 635-*quater* e 635-*qunquies* c.p.), nonché la «*frode informatica del soggetto che presta servizi di certificazione di firma elettronica*» (art. 640-*quinquies* c.p.).

A seguito della procedura di infrazione, aperta nei confronti dell'Italia dalla Commissione europea per il mancato recepimento e la non conformità della nostra legislazione alla direttiva 2013/40/UE, relativa agli attacchi contro i sistemi di informazione, il legislatore, con l'art. 19 l. 23 dicembre 2021, n. 238, recante «*disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea*», è nuovamente intervenuto nel "territorio" del diritto penale dell'informatica, novellando in modo significativo alcuni reati contro la riservatezza e la sicurezza informatiche (artt. 615-*quater*, 615-*quinquies*, 617-*quater* e 617-*quinquies* c.p.).

Con il d.lgs. 8 novembre 2021, n. 184, di «*attuazione della direttiva 2019/713/UE del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti e che sostituisce la decisione quadro 2021/413/GAI del Consiglio*», il Parlamento ha, da ultimo, modificato l'art. 493-*ter* c.p., ora rubricato «*indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti*». Ha altresì inserito, sempre tra i delitti contro la fede pubblica del titolo VII del libro II del codice penale, all'art. 493-*quater* c.p., un nuovo reato di «*detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti*».

Nel presente contributo, dopo aver definito i concetti di *cybercrime* e *Artificial Intelligence Crime* (par. 2), si verificherà se i reati cibernetici contemplati nel nostro ordinamento giuridico consentano di punire le sempre più frequenti minacce poste in essere mediante l'utilizzo abusivo dell'IA o se, trattandosi di fenomeni del tutto nuovi (*new wine in new bottles*), si debba prendere in considerazione, in prospettiva *de jure condendo*, l'opportunità di introdurre norme incriminatrici *ad hoc*. A tal fine si verificherà, sulla base di alcuni esempi concreti, se nei reati cibernetici previsti nel codice penale possano essere ricomprese, da un lato, le ipotesi in cui l'IA costituisca la peculiare modalità di esecuzione di un fatto illecito (par. 3) e, dall'altro, le aggressioni a sistemi di IA e, più in generale, alle tecnologie dell'IA (par. 4). In conclusione, si formuleranno alcune brevi considerazioni finali (par. 5).

2. Dal *Cybercrime* all'*Artificial Intelligence Crime*

Ad oggi non vi è una definizione unanime di *cybercrime*. A tale concetto vengono ricondotti, di regola, i comportamenti illeciti che possono essere commessi esclusivamente sul *web* (ad es. *phishing*, *vishing*, *pharming*, attacchi mediante *malware*) ovvero i reati che, pur non essendo connotati in sede di tipicità da elementi o "connotati" *stricto sensu* informatici, ammettono la possibilità di essere realizzati tanto *off-line* quanto *online* o comunque nel *cyberspace* (ad es. diffamazioni, *child-grooming*, truffe, violazioni del *copyright*, ecc.).

Negli ultimi anni, il rapido sviluppo dell'IA, del *Machine Learning* (ML) e delle reti neuronali artificiali ha portato alla creazione di agenti intelligenti artificiali e robot, dotati di un livello di autonomia tale da consentirgli di sostituirsi, in tutto o in parte, a molte attività dell'uomo. L'impiego, in diversi ambiti della vita quotidiana, dell'IA e della robotica, sta apportando significativi benefici alla società[1].

L'AI, configurandosi come una tecnologica c.d. a "duplice uso" (*dual-use technology*), può, però, essere impiegata dall'uomo non solo per svolgere attività lecite, ma anche, per finalità illecite[2].

Di recente, è stato coniato il concetto di *Artificial Intelligence Crime*

1) Basti pensare, ad es., all'utilizzo della robotica in ambito chirurgico (*surgical robotics*), nella cura e nell'assistenza degli anziani (*elderly care robots*), nelle attività produttive (*industrial AI*) o nella circolazione stradale (*self-driving cars*).
2) In argomento v. Trend Micro Research, *Malicious Use and Abuses of Artificial Intelligence*, 2020, consultabile sul sito *https://www.europol.europa.eu/cms/sites/default/files/ documents/malicious_uses_and_*abuses_of_artificial_intelligence_europol.pdf.

(*AI-Crime*) per abbracciare i nuovi e peculiari comportamenti criminosi posti in essere mediante agenti artificiali e robot, che possono affiancarsi o sostituirsi all'uomo nella commissione di attività illecite. In questo senso, l'IA favorisce l'emersione di nuove forme di aggressione non solo a beni giuridici tradizionali (patrimonio, vita e integrità fisica, dignità, ecc.), ma anche nuovi (ad es. riservatezza e sicurezza informatiche).

Dalle notizie di cronaca emerge come i criminali informatici stiano ricorrendo sempre più spesso alle tecnologie dell'IA per accedere abusivamente a sistemi informatici, per porre in essere attacchi sul *web*, per diffondere *malware* e *ransomware*, per manipolare l'opinione pubblica mediante *fake news*, ecc.

Tre sono i principali ambiti nei quali possono manifestarsi le minacce connesse con l'utilizzo indebito od illecito dell'IA. In primo luogo, l'AIC può mettere in serio pericolo la sicurezza cibernetica, vale a dire la riservatezza, la integrità e la disponibilità di dati e di sistemi informatici, e in specie dei sistemi che controllano le infrastrutture critiche[3]. In secondo luogo, l'AIC può costituire una seria minaccia per la sicurezza dei sistemi c.d. cyber-fisici[4]. Esso può, infine, rappresentare, più in generale, un pericolo per la collettività e l'ordine pubblico[5].

Allo stato attuale, pare difficile che un agente artificiale sia in grado di compiere autonomamente un fatto che, se realizzato da un uomo, sarebbe considerato penalmente rilevante. E in tal senso gli esperti concordano sul fatto che, ad oggi, un agente artificiale, per quanto possa essere dotato di un elevato livello di autonomia, non possa essere considerato come il vero "autore" di un reato, essendo privo di coscienza, ma soltanto come un "mezzo a delinquere". Non mancano, invece, gli esempi in cui gli agenti artificiali e le tecnologie dell'IA vengono già impiegati da soggetti malintenzionati quali strumenti per la commissione di fatti illeciti (par. 3) ovvero costituiscono oggetto di insidiose forme di aggressione (par. 4).

---

3) In argomento v. MIT Technology Review Insight, *Preparing for AI-enabled Cyberattacks*, 2021, consultabile sul sito *https://wp.technologyreview.com/wp-content/uploads/2021/04/Preparing-for-AI-enabled-attacks_final.pdf?_ga=2.121914763*.1242433566.1659528504-1380682891.1659528504.

4) L'impiego dei sistemi cyber-fisici è molto frequente nell'ambito delle telecomunicazioni, dei trasporti, del controllo intelligente del traffico, della domotica, dell'avionica, dell'industria 4.0, delle *smart-grids*, ecc.

5) Si pensi, in tal senso, all'utilizzo dell'IA per la diffusione di *fake news*, per la manipolazione dell'opinione pubblica, per la realizzazione di campagne di odio, ecc.

3. L'IA come strumento per la commissione di reati

L'impiego delle tecnologie dell'IA può innanzitutto venire in rilievo quale peculiare mezzo di esecuzione di un reato tradizionale o cibernetico. Paradigmatico è, in tal senso, il fenomeno dello *spear phishing*[6].

La condotta consistente nel procurarsi abusivamente, mediante questa sofisticata tecnica di *social engineering*, codici, parole chiave o altri mezzi idonei ad accedere ad un sistema informatico al fine di procurare a sé o ad altri un profitto potrebbe essere ricondotta nell'alveo della novellata fattispecie di «*detenzione, diffusione e installazione abusiva di apparecchiature, codici o altri mezzi atti all'accesso a sistemi informatici o telematici*» di cui all'art. 615-*quater* c.p. Nel concetto di «*mezzi idonei*» possono, infatti, essere ricomprese anche le credenziali, che consentono di accedere all'*home banking* della vittima di un attacco di *spear phishing*.

Una recente ricerca svolta dai ricercatori di due prestigiose università europee ha consentito di sviluppare, mediante l'IA e gli algoritmi di *deep Learning*, un *software* in grado di ricostruire il *pin* utilizzato da un cliente allo sportello bancomat, sebbene quest'ultimo avesse occultato il movimento delle dita sul tastierino con l'altra mano[7]. Non è da escludere che in un prossimo futuro i *cyber-criminals* possano ricorrere ad analoghi *software* per conseguire illecitamente un profitto per sé o per altri. Condotte di questo tipo, però, sono già penalmente sanzionate nel nostro ordinamento.

La fattispecie di nuovo conio di cui all'art. 493-*quater* c.p. punisce, con la reclusione fino a due anni e la multa, la produzione, la messa a disposizione o, comunque, il fatto di procurare a sé o ad altri «*dispositivi*» o programmi informatici che sono costruiti principalmente o che sono specificamente adattati per commettere reati riguardanti strumenti di pagamento diversi dai contanti[8]. La menzionata pena può applicarsi al criminale informatico che, al fine di farne

6) *Spear phishing* significa letteralmente "pesca con la lancia". Grazie all'impiego dell'IA, i criminali informatici sono in grado di studiare le abitudini, i gusti e le preferenze degli utenti sul *web*. In questo modo riescono a confezionare, mediante appositi algoritmi, mail fraudolente mirate, la cui possibilità di trarre in inganno un gruppo determinato di utenti e conseguire, mediante la loro cooperazione artificiosa, dati personali (*password*, ID, numeri di carte di credito, ecc.) è molto più alta rispetto alle tradizionali tecniche di ingegneria sociale.

7) AA.VV., *Hand Me Your PIN! Inferring ATM PINs of Users Typing with a Covered Hand*, consultabile sul sito *https://arxiv.org/abs/2110.08113*.

8) Qualche dubbio potrebbe essere sollevato rispetto alla delimitazione dell'oggetto materiale del menzionato reato, dal momento che, di regola, la tecnologia di IA ha un duplice uso. Potrebbe pertanto essere difficile dimostrare, in sede processuale, che tali *software*, come espressamente stabilito dall'art. 493-*quater* c.p., «*per caratteristiche tecnico-costruttive e di progettazione*», siano stati costruiti *principalmente* o *specificamente* adattati per commettere reati riguardanti i mezzi di pagamento diversi dai contanti. Sicuramente meglio avrebbe fatto il nostro legislatore ad incriminare i dispositivi e i programmi informatici oggettivamente *idonei* a commettere i suddetti reati.

uso nella commissione di reati aventi ad oggetti mezzi di pagamento diversi dai contanti, entri nella disponibilità di dispositivi di IA che consentano di scoprire il *pin* necessario per effettuare un prelievo allo sportello *bancomat*.

L'IA consente altresì di sviluppare nuove tecniche per facilitare lo spionaggio di dati (*cyber-espionage*), l'accesso non autorizzato a sistemi informatici (*hacking*), nonché per sferrare attacchi mirati contro determinati sistemi informatici (*cyber-attacks*)[9]. In tal senso, vi sono sempre più evidenze in merito all'impiego da parte di soggetti malintenzionati di c.d. *AI-driven malware*, particolarmente difficili da identificare e da neutralizzare da parte dei sistemi di cybersicurezza (antivirus, *firewall*, ecc.), utilizzati per realizzare *cyber-attacks* su larga scala, anche a livello internazionale.

Il criminale che disponesse senza autorizzazione di *AI-driven malware* o che abusivamente si procurasse o mettesse a disposizione di terzi suddetti *software* allo scopo di danneggiare dati o sistemi informatici potrebbe essere punito in base al delitto di «*detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*» di cui all'art. 615-*quinquies* c.p., che, come si è evidenziato in precedenza (par. 1), è stato in parte modificato dall'art. 19, co. 2, lett. b), l. n. 238/2021.

4. Le aggressioni alle tecnologie dell'IA

Gli agenti artificiali ed i sistemi di IA, pur non essendo espressamente richiamati nell'ambito delle fattispecie riconducibili al diritto penale dell'informatica, possono costituire in molti casi l'oggetto materiale di un reato, in quanto "beni" sui quali ricade il fatto di reato.

Non sussistono particolari problemi per equiparare, anche agli effetti della legge penale, gli agenti artificiali, che operano sulla base di algoritmi, ad un programma informatico. Di conseguenza, ogni fatto non autorizzato che comporti l'alterazione, la modificazione, la soppressione o il deterioramento di un agente artificiale può essere sussunto, *de jure condito*, nelle fattispecie di danneggiamento di dati e di programmi informatici "privati" o "pubblici" di cui agli artt. 635-*bis* e 615-*ter* c.p.

Gli agenti artificiali, composti da uno o più dispositivi di tipo *hardware* e *software*, possono, invece, essere equiparati ad un sistema informatico o te-

9) Sui c.d. *AI-Driven attacks* v. il *white paper* dal titolo *The Next Paradigm Shift: AI-Driven Cyber Attacks*, consultabile su *https://www.oixio.ee/sites/default/files/the_ne xt_paradigm_shift_-_ai_driven_cyber_attacks.pdf.*

lematico. Il fatto non autorizzato di distruggere, rendere, totalmente o parzialmente inservibile od ostacolare gravemente il funzionamento di un sistema di IA o di un robot acquisterebbe pertanto rilievo penale, integrando gli estremi dei reati di danneggiamento di sistemi informatici ("privati" o "pubblici") di cui agli artt. 635-*quater* e 635-*quinquies* c.p.

Dunque, in linea generale, alle aggressioni o interferenze commesse a danno di agenti artificiali possono applicarsi i reati cibernetici il cui oggetto materiale è costituito da dati ovvero sistemi informatici.

La condotta dell'*hacker* che acceda senza autorizzazione ad un sistema cyber-fisico, che controlla una infrastruttura critica, può essere ricondotta al reato di accesso abusivo ad un sistema informatico o telematico di cui all'art. 615-*ter* c.p.

Si aggiunga poi che la riconducibilità di molti agenti artificiali al concetto normativo di «*programma per elaboratore*», che viene equiparato, dall'art. 1, co. 2, l. 22 aprile 1941, n. 633 e succ. modifiche (c.d. legge sul diritto d'autore) alle opere letterarie, consente di punire la loro duplicazione e commercializzazione abusive, nonché, in forza dell'art. 171-*bis* l. cit., le condotte di fabbricazione, distribuzione o vendita di dispositivi, anche di IA, che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di protezione, destinate ad impedire o limitare atti non autorizzati dai titolari del *copyright ex* art. 171-*bis* l. cit.

5. Brevi considerazioni finali

L'incessante sviluppo dell'AI, del ML e delle reti neuronali artificiali potrebbe favorire, in un prossimo futuro, la creazione di agenti artificiali completamente autonomi ed in grado di "autodeterminarsi", di comprendere il disvalore sociale dei loro comportamenti e di realizzare condotte aventi rilievo penale. Se così fosse, il legislatore dovrebbe inevitabilmente prendere in considerazione l'opportunità, da un lato, di introdurre nuove norme incriminatrici per punire le nuove minacce a beni giuridici, meritevoli e bisognosi di tutela penale, commesse mediante le tecnologie dell'IA e, dall'altro, di prevedere per gli agenti artificiali che abbiano "consapevolmente" commesso un reato un sistema *ad hoc* di sanzioni (anche) penali.

Nell'attesa di capire se la scienza penale verrà chiamata in futuro a confrontarsi con un diritto penale per agenti artificiali, una corretta interpretazione ed applicazione dell'articolato quadro dei reati cibernetici vigenti nel nostro ordinamento consentono di evitare pericolosi vuoti di tutela e di punire coloro che sfruttino le enormi potenzialità delle tecnologie dell'IA per finalità illecite.

Bibliografia

Brennen S., *Cybercrime Metrics: Old Wine, New Bottles?*, in *Virginia Journal of Law and Technology*, vol. 9, n. 13, 2004, 1-52

Cadoppi A. - Canestrari S. - Manna A. - Papa M. (diretto da), *Cybercrime*, Milano, 2019

Cappellini A., *Machina delinquere non potest? Brevi appunti su intelligenza artificiale e responsabilità penale*, in *Discrimen*, 2019, p. 1 ss.

Crescioli C., *Le recenti modifiche ai reati cibernetici, tra tardivo recepimento delle direttive europee e nuove incriminazioni: riflessioni critiche*, in *Arch. pen*., fasc. 2, 2022, p. 1 ss.

Guembe B. et al., *The Emerging Threat of AI-driven Cyber Attacks: A Review*, in *Applied Artificial Intelligence, An Int'l Journal*, vol. 36, 2022, 1 ss.

King T.C. et al., *Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions*, in *Science and Engineering Ethics*, 2019, 1 ss.

Parodi C. - Sellaroli V. (a cura di), *Diritto penale dell'informatica. Reati della rete e sulla rete*, Milano, 2020

Philipps K. et al., *Conceptualizing Cybercrime: Definitions, Typologies, and Taxonomies*, in *Forensic Sci.*, 2022, 2, 379-398.

Piergallini C., *Intelligenza artificiale: da 'mezzo' ad 'autore' del reato?*, in *Riv. it. dir. proc. pen*., 2020, p. 1745 ss.

Salvadori I., *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale*, in *Riv. it. dir. proc. pen*., 2021, p. 83 ss.

La competenza per i "reati in rete"

di Elisabetta Ceniccola*

1. Premessa. Principi generali sulla competenza, conflitti e contrasti

Il principio del giudice naturale precostituito per legge previsto dall'art. 25, comma 1, della Costituzione fonda la necessità che la legge, e nel caso che qui ci occupa il codice di procedura penale, preveda regole che consentano l'individuazione indefettibile dell'Ufficio Giudiziario competente ad occuparsi di uno specifico procedimento/processo – cioè il Giudice (delle indagini preliminari, della cognizione o dell'esecuzione) cui il caso deve essere sottoposto – e conseguentemente l'Ufficio del Pubblico Ministero istituito presso di esso che debba condurre le indagini, esercitare l'azione penale e sostenere l'accusa in giudizio.

Giova precisare che costituisce questione assai diversa quella dell'individuazione del giudice/pubblico ministero persona fisica, incardinato presso il Tribunale o la Procura competenti, che sarà investito della trattazione di quell'affare, le cui modalità di scelta sono affidate – per il mezzo della normativa secondaria, cioè le circolari del Consiglio Superiore della Magistratura – ai progetti organizzativi elaborati periodicamente dai Capi degli Uffici giudicanti e requirenti (cd. *tabelle*). A tale fine presso detti Uffici, soprattutto se di dimensioni medio-grandi, sono previsti rispettivamente sezioni specializzate o specifici gruppi di lavoro, i cui componenti variano periodicamente e nei quali l'assegnazione dei singoli affari è assegnata in maniera tendenzialmente automatica, a rotazione.

Per quanto riguarda gli Uffici di Procura, di maggiore interesse in questa sede, oltre all'attribuzione dell'affare ad un sostituto procuratore appartenente al gruppo di specializzazione (presso la Procura della Repubblica di Roma vi è il Gruppo "Reati informatici", coordinato da un Procuratore Aggiunto), vige anche la regola del "precedente", che consente di attribuire al medesimo magistrato i procedimenti appartenenti al medesimo filone di indagine, in ragione della omogeneità delle modalità operative adoperate dall'autore del fatto, della categoria delle persone offese prese di mira, ovvero dell'identità dell'autore stesso (una sorte di recupero del criterio della competenza per connessione ex art. 12 c.p.p. esteso alla connessione probatoria).

Per tornare alla tematica della competenza in senso proprio ed eviden-

(*) Sostituto Procuratore Generale della Procura Generale presso la Corte di Cassazione.

ziare la rilevanza che la stessa riveste, è opportuno ricordare che l'ordinamento prevede, come correttivo all'errata o dubbia applicazione delle norme che la regolano, la possibilità di sollevare un conflitto o contrasto, positivo o negativo, di competenza, nel caso in cui vi siano divergenze tra autorità giudiziarie.

Si parla di conflitto di competenza laddove siano due giudici a rivendicare o a ricusare la competenza su di un affare (art. 28 e segg. c.p.p.); si parla di contrasto laddove siano più uffici di procura a rivendicare o a ricusare la competenza di un medesimo affare (art. 54 e segg. c.p.p.): i primi sono sollevati nelle fase processuale o procedimentale in cui l'affare si trova *sub iudice*, i secondi nel corso delle indagini preliminari, ed, più in particolare quando un giudice non abbia ancora avuto modo di pronunciarsi sulla competenza.

Ulteriormente, il conflitto o il contrasto si dice positivo quando due giudici o pubblici ministeri si ritengono entrambi competenti, al contrario, negativo quando entrambi i giudici o pubblici ministeri si ritengono non competenti.

La risoluzione dei conflitti di competenza è attribuita alla Corte di Cassazione (art. 32 c.p.p. e, in particolare, le *tabelle* della Corte di Cassazione ne assegnano la soluzione alla Prima Sezione penale), che vi provvede con sentenza. Purtuttavia, quando una questione di competenza sorta nell'ambito di un processo o procedimento non sia stata oggetto di conflitto e di remissione diretta alla Corte di Cassazione, la risoluzione è lasciata ai giudici della cognizione ed, eventualmente, giungerà all'esame della Corte di Cassazione solo se oggetto di ricorso (in questo caso la decisione è attribuita a quella sezione della Corte di Cassazione cui le *tabelle*, attribuiscono la trattazione dei ricorsi per lo specifico tipo di reato oggetto del processo).

Specularmente, alle Procure Generali presso le Corti d'Appello ed alla Procura Generale presso la Corte di Cassazione, ex art. 54, 54-*bis*, 54-*ter* c.p.p., spetta rispettivamente il compito di dirimere, mediante decreto, i contrasti positivi o negativi di competenza sorti tra pubblici ministeri il cui Ufficio si trova nello stesso distretto di Corte d'Appello, ovvero in diversi distretti di Corte d'Appello, nonché, ex 54-*quater* c.p.p., di pronunciarsi sulle istanze di trasmissione per competenza avanzata da una delle parti private, che l'ufficio del pubblico ministero che sta conducendo le indagini non ha accolto o sulle quali non si è pronunciato entro dieci giorni.

Appare, poi, rilevante ricordare che il progetto organizzativo – cd. *tabelle* – della Procura Generale presso la Corte di Cassazione prevede da anni un gruppo specializzato di Sostituti Procuratori Generali coordinati da un Avvocato generale o da un Sostituto esperto, che, tendo conto delle pronunce

della Corte di Cassazione, assume decisioni volte ad assicurare coerenza ed unitarietà nell'applicazione delle norme sulla competenza negli Uffici requirenti, secondo la funzione nomofilattica precipua degli Uffici di legittimità.

La Procura Generale, proprio al fine di evitare inutile dispendio di tempo ed energie ha pubblicato sul sito web, a disposizione di chiunque vi abbia interesse, gli orientamenti dell'ufficio in materia di contrasti[1], aggiornati da ultimo nel dicembre 2022, che costituiscono un valido vademecum per le Procure della Repubblica e, ancor prima, per la Polizia Giudiziaria che a queste ultime ha il compito di inoltrare le notizie di reato.

Gli orientamenti, che non pretendono di essere un trattato esaustivo della casistica in materia di competenza, si soffermano su quelle fattispecie che presentano questioni interpretative di maggiore difficoltà, rilevanza o diffusione.

Si tratta di un supporto di agile consultazione, la cui estrema utilità si apprezza ponendo mente alla circostanza che la pendenza del contrasto di competenza non costituisce causa di sospensione né del termine di prescrizione del reato, né del termine per lo svolgimento delle indagini preliminari, laddove l'immediata corretta individuazione dell'Ufficio di Procura che deve procedere consente di dedicare proficuamente il termine previsto dalla legge allo svolgimento dell'attività di indagine in senso tecnico.

Il fattore tempo, peraltro, proprio per la *volatilità* dei dati, delle informazioni e delle pubblicazioni in *rete*, gioca un ruolo determinante per le indagini in campo di reati, anche latamente intesi, informatici.

È rilevante, poi, chiarire che lo spartiacque tra l'investitura della Corte di Cassazione in sede di conflitto e quella delle Procure generali in sede di contrasto è costituito dalla sottoposizione o meno della *res judicanda* ad un giudice, da parte dell'Ufficio requirente che se ne occupa.

Ciò comporta che dopo l'esercizio dell'azione penale o la richiesta di archiviazione indubbiamente spetta al giudice pronunciarsi sulla competenza ed, eventualmente, investire (anche a seguito di sollecitazione delle parti processuali) la Corte di Cassazione in caso di conflitto, e, d'altra parte, che non sempre in fase di indagini preliminari il pubblico ministero o la parte privata, ex art. 54-*quater* c.p.p., possano rivolgersi alle Procure Generali in sede di contrasto. Laddove, infatti, il pubblico ministero abbia già in fase di indagini preliminari investito un giudice – ad esempio con una richiesta cautelare – e questo si sia già anche implicitamente dichiarato competente o esplicitamente incompetente, non vi è più spazio per un contrasto o per la

1) *Https://www.procuracassazione.it/procura-generale/it/intro_penale.page*: "La risoluzione dei contrasti".

richiesta di trasmissione degli atti ad altro Ufficio di Procura ad iniziativa di una parte privata.

Tuttavia, le decisioni assunte per la determinazione della competenza in fase di indagini preliminari hanno validità *rebus sic stantibus*, proprio per la fluidità che caratterizza la contestazione (fino alla cristallizzazione nell'atto con cui si esercita l'azione penale), e sono suscettibili di rivalutazione nel caso di riqualificazione giuridica del fatto o anche con l'ampliamento delle indagini e l'individuazione di ulteriori e, soprattutto, più gravi reati. In tal caso la decisione può essere nuovamente rimessa alla Procura Generale distrettuale o di legittimità.

Da ultimo, appare opportuno sottolineare, come già accennato, che il principio del giudice naturale e le regole sulla competenza che ne discendono rivestono una importanza tale che l'errata impostazione iniziale sull'Ufficio da investire si riverbera su tutto il processo, poiché può determinare l'estinzione del reato per decorso del termine di prescrizione o l'annullamento dei processi, con maggiore probabilità, proprio in ragione della enorme pendenza del contenzioso, di declaratoria di improcedibilità ai sensi dell'art. 344-*bis* c.p.p., introdotta dall'art. 2, comma 2, lettera a) della l. n. 134/2021, cd. riforma Cartabia.

È vero, infatti, che la questione sulla competenza (quella territoriale, se tempestivamente sollevata, e quella funzionale, anche ove non sollevata, perché rilevabile d'ufficio), se ritenuta fondata in sede di appello o di ricorso per cassazione, determina l'annullamento dei provvedimenti adottati e la necessità che il processo ricominci daccapo.

2. I reati in rete. Concetto

La perimetrazione dell'argomento necessita di un succinto chiarimento di diritto sostanziale, ovvero di ciò che si intende per "*reati in rete*" o "*reati informatici*" o ancora "*cybercrimes*" o "*computer crime*".

Si tratta di una categoria generale di reati in continua espansione, addirittura esponenziale negli ultimi decenni, in considerazione della rapidità con cui si è diffusa la rete internet e le sue piattaforme, con cui sono proliferati i social sempre più frequentati, con cui la tecnologia ad essi sottostante si è evoluta, nonché con l'esorbitante numero dei fruitori: un fenomeno ormai dilagante e fuori controllo.

Non esiste, pertanto, una definizione universalmente riconosciuta dei *reati in rete*, anche se l'Unione europea, considera *cybercrime*: "*any criminal*

acts associated with computers, networks, ICT and online activity"[2], che, alla luce delle tradizionali categorie del reato, potrebbe essere tradotto come "*delitto commissivo punibile a titolo di dolo in danno o per mezzo della tecnologia dell'informazione (sistema informatico o telematico, dati, informazioni, programmi)*".

Ciò che si può affermare, però, è che nella categoria dei "*reati in rete*" si riconoscono due specie: i reati informatici *stricto sensu* e i reati informatici *lato sensu*.

Tra i primi rientrano quei reati il cui presupposto indefettibile è l'utilizzo del mezzo informatico (il computer o qualsiasi altro dispositivo elettronico che consente l'accesso alla rete) e per i quali, tendenzialmente, la rete stessa e i sistemi informatici ad essa collegati rappresentano l'obiettivo della condotta illecita, in sostanza esistono esclusivamente perché esistono i sistemi informatici.

Nei secondi, al contrario, si annoverano numerosi reati comuni – che aggrediscono i tradizionali beni giuridici, come riservatezza, patrimonio, domicilio, fede pubblica, ecc. – occasionalmente commessi con il mezzo informatico, i quali appunto hanno subìto una trasformazione e diffusione proprio grazie alla tecnologia informatica, in progressiva e continua evoluzione. È sufficiente pensare ai reati di diffamazione, molestia, violenza sessuale, *stalking*, truffa, riciclaggio (attuato con le piattaforme di gioco *online*)[3], ecc., per comprendere i risvolti negativi dello sviluppo dell'informatica e della telematica, che contraggono i tempi di svolgimento di attività commerciali o informative (e-commerce, e-government, home-banking, trading on line), abbattono le frontiere e rendono volatile qualsiasi aggancio territoriale o anche personale (l'agente in molti casi non corrisponde al titolare della connessione da cui opera)[4].

---

2) *Https://www.iss.europa.eu/sites/default/files/EUISSFiles/Report_21_Cyber.pdf.*

3) G. Panucci, *Reati informatici e mezzi di ricerca della prova*, SSM Struttura didattica decentrata della C.A. di Catanzaro "Criminalità informatica e tecniche di investigazione" , Tribunale di Cosenza, 15.12.2021, interessante per la descrizione della fattispecie, esemplificativo della difficoltà nell'individuazione della competenza territoriale: "*Sulla piattaforma di gioco vengono creati due conti gioco intestati ad identità fittizie. Ad usarli è la stessa persona oppure due persone in accordo tra loro. Dei due, uno viene caricato coi proventi da riciclare; l'altro invece con il denaro strettamente necessario a partecipare. Sulla piattaforma i due conti gioco entrano sullo stesso tavolo virtuale (il gioco più gettonato è quello del poker on line) e dei due uno (quello vuoto) gioca a vincere e l'altro (quello su cui è depositata la provvista da ripulire) gioca a perdere. In questo modo viene realizzata una traslazione informatica di denaro apparentemente lecita tra due conti gioco di cui l'uno si svuota e l'altro si riempie, con successiva monetizzazione da parte di quest'ultimo con le forme di riscossione delle vincite previste dalla piattaforma*".

4) G. Specchio, Ten. CC Ph.D., *Analisi di contesto del cyberspace*, Scuola Superiore della Magistratura (SSM), formazione decentrata della Corte d'Appello di Roma, Roma, 19 settembre 2019, in "Le condotte ingannevoli nel sistema del diritto penale" che, dal punto di vista più operativo,

Assai opportuna, sul punto, è la considerazione che la difficoltà del legislatore, dovuta alla velocità di diffusione dei fenomeni in rete, di approntare tempestivi strumenti di protezione e di repressione efficaci e aggiornati rispetto all'evolversi delle tecnologie e delle nuove forme di criminalità, non può che essere compensata con la necessità che l'interprete – operatore giudiziario – che ha diretto e quotidiano contatto con la fenomenologia, colmi i vuoti con uno sforzo ermeneutico atto a ricondurre le condotte nuove e tecnicamente sofisticate nell'alveo degli strumenti esistenti[5].

---

rappresenta che enti quali Interpol e Europol - EC3 distinguono:
- reati commessi in danno dei sistemi informatici e telematici, detti anche *advanced cybercrime* (oppure *high-tech crime* o *cyber-dependent crime*), come ad esempio condotte commesse mediante tecniche di hacking (D-DOS, Botnet, Zombi, ecc.), *crimeware* (Virus, Worm, Trojan, ecc.), *spamming*, ecc.;
- reati commessi per mezzo dei sistemi informatici e telematici, detti anche *cyber-enabled crime*, come ad esempio reati in materia di pornografia minorile, reati finanziari, terrorismo, atti persecutori, ecc.

5) I.M. Allieri, referente per il settore penale, *Brevi note introduttive*, SSM Struttura didattica territoriale C.A. L'Aquila "I reati commessi con l'uso dei sistemi informatici e telematici", Tribunale di Pescara, 24 giugno 2016.
Si riporta di seguito uno stralcio della relazione, che in maniera schematica ripercorre le tappe con le quali il legislatore si è via via adeguato alle nuove realtà: «*Com'è noto, il legislatore penale nazionale, si è dovuto adeguare a tale rapido e dilagante fenomeno, reso esponenziale in particolare dall'avvento di internet, peraltro in continuo divenire. Excursus normativo. Dapprima, anche in seguito alla raccomandazione del Consiglio d'Europa n. 89 del 9 settembre 1989 e con la legge 547/1993 "Modificazioni ed integrazioni delle norme del codice penale e del codice di procedura penale in tema di criminalità informatica", ha introdotto una prima normativa organica, creando nuove fattispecie di reato disseminate all'interno del codice penale (e non raggruppate in una specifica sezione), a riprova del fatto che i medesimi beni giuridici (riservatezza, patrimonio, domicilio, fede pubblica) potevano essere oggi aggrediti con nuovi e più raffinati strumenti ed estendo la tutela non solo al sistema informatico, ma anche telematico.*
Quindi è stata introdotta una tutela non solo del sistema informatico, ma anche telematico.
Ad esempio, l'art. 392 c.p. esercizio arbitrario delle proprie ragioni in cui la violenza sulle cose può essere integrata dall'alterazione di un programma informatico ovvero mediante il turbamento di un sistema informatico o telematico, l'art. 420 c.p. attentato a impianti di pubblica utilità, danneggiamento di sistemi informatici o telematici di pubblica utilità, art. 491 c.p. falsità del documento informatico pubblico o privato, art. 615-bis c.p. accesso abusivo ad un sistema informatico o telematico, 615-quater detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici, 615-quinquies diffusione di programmi diretti a danneggiare o interrompere un sistema informatico, 617-quater intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche, 635-bis danneggiamento di sistemi informatici o telematici, 640 ter c.p. frode informatica.
È stato emanato il Codice in materia di protezione dei dati personali (D.lgs. 30 giugno 2003 n. 196, con l'introduzione di specifiche ipotesi sanzionatorie quali il trattamento illecito dei dati).
Con la legge 48/2008 di ratifica della Convenzione del Consiglio d'Europa siglata a Budapest nel 2001 (primo accordo europeo sulla criminalità digitale) è stata ulteriormente potenziata la disciplina sanzionatoria, con la previsione di ipotesi integrative quali il falso informatico, 491-bis c.p., danneggiamento informatico, 635-bis, ter, quater, quinquies).
Con la legge 38/2006 è stata disciplinata e sanzionata la diffusione, anche a mezzo internet, di immagini pedopornografiche [...].
Anche il tradizionale schema del reato di truffa è apparso inadeguato alle nuove condotte on line ed è stato necessario introdurre il reato di frode informatica di cui all'art. 640 ter c.p.
Tale fattispecie, costruita come autonoma e distinta dalla semplice truffa, è stata introdotta,

3. La giurisdizione e la competenza dei reati in rete. Generalità

La prima immediata considerazione, rappresentata da alcuno in maniera icastica, è che la difficoltà nell'approccio con i reati informatici risiede nel carattere smaterializzato, ubiquo ed istantaneo delle comunicazioni/operazioni informatiche, sicché le fattispecie criminose sono intrinsecamente transnazionali ed istantanee[6].

Ciò evidenzia con immediatezza l'ossimoro che risiede nella locuzione "competenza territoriale dei reati informatici", atteso che il concetto di competenza territoriale, ed ancor prima quello di giurisdizione che consente l'applicazione della legge nazionale, evoca l'esistenza di un luogo fisico che rientra nel circondario di un Tribunale, mentre l'essenza dei *cybercrimes* risiede in uno spazio virtuale, che si giova proprio di tutte le prerogative della rete virtuale in termini di delocalizzazione delle condotte e degli eventi, della possibilità che condotta ed evento siano tra loro sincroni o asincroni. Tale inconciliabilità è superabile esclusivamente con una duplice *fictio*: considerare lo spazio virtuale quale spazio materiale[7] ed agganciarlo al territorio,

---

come può leggersi nella Relazione alla legge 547/1993, per superare la difficoltà derivante dal fatto che la truffa è sempre stata intesa nell'ambito di una relazione intersoggettiva, atteso che gli artifizi e i raggiri sono di norma indirizzati a condizionare il consenso umano; invece, nel caso di frode informatica, il contegno del soggetto passivo è irrilevante.

Anzi, la frode informatica può essere integrata dalla manomissione di un bancomat o di prelievo ai danni di un conto on line, casi in cui il soggetto passivo non viene direttamente ingannato o raggirato, né può affermarsi che ad essere raggirato sia l'elaboratore elettronico, non essendo in grado di fornire alcun consenso, tantomeno un consenso viziato (talché tra frode informatica e truffa intercorre un rapporto di specialità).

L'attenzione dell'interprete si è rivolta anche alle nuove forme di comunicazione, talché appare ormai pacifico in giurisprudenza che l'utilizzo di messaggi Whats app, sms, diffusione a mezzo internet (per esempio attraverso sistemi peer to peer) di immagini, video condivisi possono rappresentare lo strumento per commettere reati di stalking, di diffamazione, ecc.».

6) Così A. Cappellini, *La cooperazione giudiziaria e di polizia. Il secondo protocollo addizionale alla Convenzione di BUDAPEST*, in una slide in occasione del Corso Vittorio Occorsio "Criminalità informatica e intelligenza artificiale", Roma, Scuola di Perfezionamento per le Forze di Polizia, sessione mattutina del 17.05.2022.

7) Cfr. Cass., sez. VI, n. 3067 del 04/10/1999, dep. 14/12/1999, Rv. 214946, secondo cui "*... deve ritenersi 'domicilio informatico', ... quello spazio ideale (ma anche fisico in cui sono contenuti i dati informatici) di pertinenza della persona, cui si estende la tutela della riservatezza della sfera individuale, quale bene anche costituzionalmente protetto*"; Cass., sez. 5, n. 13057 del 28/10/2015, dep. 31/03/2016, Rv. 266182: "*Integra il reato di cui all'art. 615 ter cod. pen. la condotta di colui che accede abusivamente all'altrui casella di posta elettronica trattandosi di una spazio di memoria, protetto da una password personalizzata, di un sistema informatico destinato alla memorizzazione di messaggi, o di informazioni di altra natura, nell'esclusiva disponibilità del suo titolare, identificato da un account registrato presso il provider del servizio (In motivazione la Corte di Cassazione ha precisato che anche nell'ambito del sistema informatico pubblico, la casella di posta elettronica del dipendente, purché protetta da una password personalizzata, rappresenta il suo domicilio informatico sicché è illecito l'accesso alla stessa da parte di chiunque, ivi compreso il superiore gerarchico)*".

Come ricorda Giorgio Panucci, op. cit.: «Altra questione in cui si è imbattuta la giurisprudenza

ove possibile con le regole principali sulla competenza dettate dall'art. 8 cod. proc. pen., ovvero con le regole suppletive di cui all'art. 9 cod. proc. pen., sulla scorta della lapalissiana osservazione che l'autore del reato non può che essere una persona fisica (un discorso a parte va fatto per la responsabilità amministrativa degli enti per gli illeciti amministrativi dipendenti da reato, ai sensi del d.lgs. n. 231/2001, in cui rientrano anche reati informatici in senso proprio e lato).

È vero, infatti, che gran parte delle soluzioni adottate dalla giurisprudenza si fonda su di una *fictio* e, in caso di incertezze nell'individuazione del luogo di consumazione dei reati, si affida alle regole suppletive previste dall'art. 8 cod. proc. pen. (del luogo in cui è avvenuta una parte dell'azione o dell'omissione) e dall'art. 9 cod. proc. pen. (residenza, domicilio o dimora dell'imputato, infine del luogo in cui ha sede l'ufficio del pubblico ministero che ha provveduto per primo a iscrivere la notizia di reato).

La preliminare problematica della giurisdizione è risolta, invece, in maniera soddisfacente dall'ordinamento che ha accolto la regola dell'ubiquità e considera commesso nello Stato un reato tanto se nel territorio nazionale si è realizzata l'azione o l'omissione, tanto se si è verificata almeno una parte della condotta o dell'evento (art. 6 cod. pen.).

Si applicheranno, pertanto, le disposizioni del codice penale e del codice di rito, tanto nell'ipotesi in cui l'agente operi uno scambio di dati tra sistemi informatici esistenti nel territorio nazionale, quanto nel caso in cui nello

---

di legittimità, con riferimento alla fattispecie di cui all'art. 600-*quater* cod. pen. concerne lo spazio di cloud, inteso come spazio virtualmente rilevante per la "detenzione" virtuale di materiale illecito». Cfr. Cass., sez. 3, n. 20890 del 11/01/2017 Ud., dep. 03/05/2017, Rv. 270125: "*Integra il delitto di detenzione di materiale pedopornografico la detenzione di cosiddetti temporary internet files, che si ottengono attraverso visite compiute dall'utente di internet su siti contenenti materiale pornografico infantile, dato che, in forza di alcuni comandi informatici, talune immagini visualizzate sul monitor, rimangono immagazzinate per un apprezzabile arco temporale nella cartella denominata, per l'appunto, temporary internet files, risultando a tutti gli effetti detenuti dall'utilizzatore; ne consegue che il detentore potrà eccepire l'esonero della responsabilità solo nel caso in cui non abbia avuto la consapevolezza dell'esistenza di files acquisiti nel corso della navigazione su internet*". Quindi, si può "detenere" materiale informatico illecito non soltanto se salvato nella memoria fissa del proprio P.C., ma anche su spazio virtuale presente in rete, di cui il P.C. conservi traccia di accesso mediante i c.d. *temporary internet files*. L'orientamento ben si presta ad essere applicato anche a maggior ragione per gli spazi di cloud, ossia al materiale informatico illecito custodito nel cloud (pensiamo ad es. a onedrive), soprattutto perché ad accesso limitato al titolare tramite chiavi di accesso username e password con effettiva possibilità di esercizio del c.d. *ius excludendi alios*.

In diversi altre occasioni in cui la Procura Generale presso la Corte di Cassazione è stata chiamata a risolvere un contrasto di competenza tra Uffici requirenti, è stato riutilizzato il concetto del domicilio informatico: «*Assume dunque rilievo, ai sensi e per i fini di cui all'art. 8 c.p.p., il luogo ove è stata attivata la carta prepagata e si trova il "conto" ad essa collegato, identificabile tramite il relativo "codice univoco" e qualificabile come vero e proprio "domicilio informatico" dell'apparente creditore, indagato quale truffatore*» (Decreto n. 223/2014).

Stato si realizzi soltanto una parte della condotta o dell'evento, mentre l'altra parte costitutiva del reato venga posta in essere all'estero. Sicché per radicare la potestà punitiva nazionale occorre che un frammento del complessivo comportamento delittuoso o un riflesso del reato si siano verificati nello Stato, come più volte affermato dalla giurisprudenza di legittimità[8].

Una ulteriore estensione della giurisdizione italiana è realizzata dall'art. 604 cod. pen., come sostituito dall'art. 10 l. n. 269/1998, secondo il quale i delitti violenza sessuale, atti sessuali con i minorenni, adescamento di minori, a fini di prostituzione e pornografia (che rientrano, ove commessi con strumenti informatici o telematici, tra reati informatici in senso lato), sono punibili secondo la legge nazionale anche quando il fatto è commesso all'estero da cittadino italiano, ovvero in danno di cittadino italiano, ovvero dallo straniero in concorso con cittadino italiano.

Da ultimo, si ricorda che per i delitti comuni commessi completamente all'estero l'art. 10 cod. pen. prevede, in presenza di specifici presupposti, l'applicazione della legge italiana quando gli stessi siano commessi in danno dello Stato o di un cittadino.

4. La competenza per i reati in rete in fase di indagini

L'esigenza di assicurare immediatezza, coerenza e completezza nelle indagini per fenomeni di rilevante allarme sociale, molto spesso gestiti da associazioni criminali o di più difficile disvelamento o di maggiore estensione territoriale, ha imposto di operare uno sganciamento della competenza dell'Ufficio Requirente da quella dell'Ufficio Giudicante, operante in maniera assoluta per la fase delle indagini e temperata per la fase dibattimentale.

L'art. 51, comma 3-*quinquies*, cod. proc. pen., infatti, attribuisce la competenza investigativa – non dell'organo giudicante, per il quale si appli-

8) Cass., sez. V, n. 4741 del 17/11/2000, dep. 27/12/2000, Rv. 217745: "*Il giudice italiano è competente a conoscere della diffamazione compiuta mediante l'inserimento nella rete telematica (internet) di frasi offensive e/o immagini denigratorie, anche nel caso in cui il sito web sia stato registrato all'estero e purché l'offesa sia stata percepita da più fruitori che si trovino in Italia; invero, in quanto reato di evento, la diffamazione si consuma nel momento e nel luogo in cui i terzi percepiscono la espressione ingiuriosa*"; Cass., sez. IV, n. 40903 del 28/06/2016 dep. 30/09/2016, Rv. 268230: "*In tema di intercettazione di comunicazioni informatiche, è legittima l'acquisizione tramite la procedura dell'istradamento dei messaggi di posta elettronica, in entrata e in uscita, relativi ad una casella gestita da un provider estero (In motivazione la Corte ha precisato che il ricorso a tale tecnica non comporta la violazione delle norme sulle rogatorie internazionali, in quanto, in tal modo, tutta l'attività d'intercettazione viene interamente compiuta nel territorio italiano, né dell'art. 8 della CEDU come interpretato dalla sentenza della Corte EDU nel caso Capriotti c. Italia)*".

cheranno le regole ordinarie tanto in fase cautelare, che di cognizione ed esecuzione – ad un ampio elenco di reati informatici, in senso proprio ed in senso lato, alle Procure della Repubblica distrettuali, cioè quelle che hanno sede nei capoluoghi di distretto. Ciò è a dirsi per i reati di cui agli artt. 414-*bis*, 600-*bis*, 600-*ter*, 600-*quater*, 600-*quater*.1, 600-*quinquies*, 609-*undecies*, 615-*ter*, 615-*quater*, 615-*quinquies*, 617-*bis*, 617-*ter*, 617-*quater*, 617-*quinquies*, 617-*sexies*, 635-*bis*, 635-*ter*, 635-*quater*, 640-*ter* e 640-*quinquies* del codice penale.

La norma prevede, poi, la possibilità che per giustificati motivi, su richiesta del Procuratore Distrettuale, con provvedimento del Procuratore Generale presso la Corte d'Appello, le funzioni di pubblico ministero per il dibattimento siano esercitate da un magistrato designato dal Procuratore della Repubblica presso il giudice competente (cd. istituto della applicazione).

Solo di seconda intenzione il legislatore, nel convertire con modificazioni il d.l. n. 92/2008 recante misure urgenti in materia di sicurezza pubblica, la legge n. 125/2008, all'art. 2, co. 1, lettera a), ha colmato la precedente lacuna normativa, aggiungendo il comma 1-*quater* all'art. 328 c.p.p., e prevedendo, quindi, che per i delitti indicati nell'art. 51, comma 3-*quinquies*, le funzioni di giudice per le indagini preliminari e le funzioni di giudice per l'udienza preliminare siano esercitate, salve specifiche disposizioni di legge, da un magistrato del Tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente, così riallineando Ufficio requirente ed Ufficio giudicante.

Da ultimo, anche ai fini della determinazione della competenza per connessione ai sensi dell'art. 16 cod. proc. pen., si sottolinea che l'art. 51, comma 3-*quinquies*, cod. proc. pen., come l'art. 51, comma 3-*bis* cod. proc. pen., "*comporta una deroga assoluta ed esclusiva alle regole sulla competenza per territorio, anche fuori dagli ambiti distrettuali, perché stabilisce la vis attractiva del reato ricompreso nelle attribuzioni di quell'ufficio inquirente nei confronti dei reati connessi anche se di maggiore gravità, con la conseguenza che, ai fini della determinazione della competenza, occorre avere riguardo unicamente al luogo di consumazione del reato previsto nel catalogo suindicato (Sez. 1, n. 43599 del 05/07/2017, Confl. comp. in proc. Di Palma, n. m.; Sez. 4, n. 4484 del 09/12/2015, dep. 2016, Rv. 265944; Sez. 2, n. 6783 del 13/11/2008, dep. 2009, El Abbouli, Rv. 243300)*" (In motivazione Cass. Sez. 1, n. 16123 del 12/11/2018, dep. 12/04/2019, Rv. 276391; conf. Cass. Pen. Sez. 1, n. 32765 del 03/05/2016, dep. 27/07/2016, Rv. 267503 - 01: «*In tema di competenza per territorio determinata da connessione, il procedimento relativo ad un reato ricompreso nell'elencazione nell'art. 51, comma terzo-bis*

e comma terzo quinquies, cod. proc. pen. esercita una "vis attractiva" rispetto ai procedimenti relativi ad altri reati ad esso connessi, anche quando tali reati siano più gravi del primo, in deroga alla previsione contenuta nell'art. 16, comma primo, cod. proc. pen.»).

5. La competenza territoriale per i reati in rete "in senso stretto". Casistica

Come già detto, l'interprete ha incontrato la difficoltà di coniugare le peculiarità del reato commesso con il mezzo informatico o telematico con le tradizionali categorie della teoria generale del reato e con i consueti istituti di diritto processuale penale.

Il reato informatico, infatti, "nella maggior parte dei casi, si realizza in remoto, a distanza, in presenza di un collegamento telematico tra più sistemi informatici con l'introduzione illecita, o non autorizzata, di un soggetto, all'interno di un elaboratore elettronico, che si trova in luogo diverso da quello in cui è situata la banca-dati". Sicché «nel *cyberspace* i criteri tradizionali per collocare le condotte umane nel tempo e nello spazio entrano in crisi, in quanto viene in considerazione una dimensione "smaterializzata" (dei dati e delle informazioni raccolti e scambiati in un contesto virtuale senza contatto diretto o intervento fisico su di essi) ed una complessiva "delocalizzazione" delle risorse e dei contenuti (situabili in una sorte di meta-territorio)». Inoltre, "la dimensione aterritoriale si è incrementata da ultimo con la diffusione dei dispositivi mobili (tablet, smartphone, sistemi portatili) e del *cloud computing*, che permettono di memorizzare, elaborare e condividere informazioni su piattaforme delocalizzate dalle quali è possibile accedere da qualunque parte del globo…"[9].

La prima e più interessante questione risolta dalla giurisprudenza di legittimità, che si è pronunciata a Sezioni Unite[10], riguarda la fattispecie di cui all'art. 615-*ter* cod. pen., *accesso abusivo a sistema informatico*, in quanto i principi affermati hanno successivamente costituito la direttrice per la soluzione da adottare per tutti i *reati in rete* – cioè per tutte le ipotesi di reato poste in essere attraverso lo strumento informatico – di mera condotta. La duttilità

9) Cass., sez. un., sent. n. 17325 del 26/03/ 2015, dep. 24/04/2015, Confl. comp. in proc. Rocco, Rv. 263020.

10) Cass., sez. un., sent. n. 17325/2015, cit., in un caso di abusiva e ripetuta introduzione nel sistema informatico del Ministero delle Infrastrutture e dei Trasporti da parte di una dipendente che era solita effettuare visure per conto di un terzo, amministratore di un'agenzia di pratiche automobilistiche.

della soluzione discende proprio dalla natura della fattispecie considerato che la condotta si esaurisce nello spazio virtuale della rete, con la necessità di individuare il luogo fisico della consumazione del reato previsto dal criterio primario di cui all'art. 8, comma 1, cod. proc. pen. Il quesito sottoposto alle Sezioni Unite[11] poneva l'alternativa tra "il luogo in cui si trova il soggetto che si introduce nel sistema o, invece, quello nel quale è collocato il server che elabora e controlla le credenziali di autenticazione fornite dall'agente".

Il primo e più risalente orientamento, che individuava la competenza nel luogo dove materialmente è collocato il server che elabora e controlla le credenziali di autenticazione del cliente[12], tra gli altri, aveva creato il problema dell'accertamento del luogo fisico di collocazione del server. Essendo il web un "mare" globale e mondiale, molti di questi server hanno sede fisica all'estero, non sempre resa nota o conosciuta, perché privati (es. *Apple* non pubblicava il luogo di collocazione dei server dei propri cloud; i cui server di *Facebook* e *Google* sono stati stabili per lunghissimo tempo solo negli Stati Uniti).

Per altro verso la soluzione portava a conseguenze incongrue perché nel caso di connessione dal territorio nazionale con accesso abusivo sul profilo *facebook* di un terzo, magari della stessa città, avrebbe comportato la consumazione del reato negli USA, oggi in Irlanda, dove sono stati spostati i server.

La soluzione maggioritaria, poi preferita dalle Sezioni Unite, afferma che «*in tema di acceso abusivo ad un sistema informatico o telematico, il luogo di consumazione del delitto di cui all'art. 615-ter cod. pen. coincide con quello in cui si trova l'utente che, tramite elaboratore elettronico o altro dispositivo per il trattamento automatico dei dati, digitando la "parola chiave" o altrimenti eseguendo la procedura di autenticazione, supera le misure di sicurezza apposte dal titolare per selezionare gli accessi e per tutelare la banca-dati memorizzata all'interno del sistema centrale ovvero vi si mantiene eccedendo i limiti dell'autorizzazione ricevuta (In motivazione la Corte ha specificato che il sistema telematico per il trattamento dei dati condivisi tra più postazioni è unitario e, per la sua capacità di rendere disponibili le informazioni in condizioni di parità a tutti gli utenti abilitati, assume rilevanza il luogo di ubicazione della postazione remota dalla quale avviene l'accesso e non invece il luogo in cui si trova l'elaboratore centrale)*»[13]. Ciò è a dirsi

11) Sez. 1, ord. n. 52575 del 28/10/2014, dep. 18/12/2014.

12) Sez. 1, n. 40303 del 27/05/2013, dep. 27/09/2013, Rv. 257252 (Fattispecie relativa ad accesso abusivo allo SDI da terminale ad esso collegato situato in Firenze, nella quale la Corte ha ritenuto di individuare il "locus commissi delicti" in Roma, dove ha sede il server).

13) G. Panucci, op. cit., puntualizza: «*Per esemplificare in estrema sintesi il ragionamento eseguito dalla Suprema Corte, si è partiti dall'art. 1 della Convenzione europea di Budapest del 23 no-*

anche nel caso di accesso mediante rete Wi-Fi pubblica o privata.

L'utilità del principio è percepibile nel caso degli attacchi informatici eseguiti tramite le c.d. *botnet*, divenute famose con *Anonymous* (associazione per delinquere di hackers dedita agli attacchi informatici ai siti istituzionali dello Stato)[14].

Se non è possibile individuare la postazione da cui agisce l'operatore tramite il *client* (computer connesso tramite rete ad un elaboratore centrale, *server*), allora potrà farsi ricorso alle regole suppletive di cui all'art. 9 cod. proc. pen.

Come ricostruito negli orientamenti per i contrati dalla Procura Generale presso la Corte di Cassazione, il reato di *frode informatica*, di cui all'art. 640-*ter* cod. pen., ha la medesima struttura e quindi i medesimi elementi costitutivi della truffa dalla quale si differenzia solamente perché l'attività fraudolenta dell'agente investe non la persona (soggetto passivo), di cui difetta l'induzione in errore, bensì il sistema informatico di pertinenza della medesima, attraverso la manipolazione di detto sistema.

---

vembre 2001, che definisce il sistema informatico "qualsiasi apparecchiatura o gruppi di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica dei dati". Ne consegue che lo spazio informatico di più sistemi interconnessi anche via web deve essere guardato in maniera unitaria. In questo "spazio virtuale", l'azione telematica viene realizzata attraverso una connessione tra sistemi informatici distanti tra loro, cosicché gli effetti della condotta possono esplicarsi in un luogo diverso da quello in cui l'agente si trova; inoltre, l'operatore, sfruttando le reti di trasporto delle informazioni, è in grado di interagire contemporaneamente sia sul computer di partenza sia su quello di destinazione. La nozione di collocazione spaziale o fisica è essenzialmente estranea alla circolazione dei dati in una rete di comunicazione telematica e alla loro contemporanea consultazione da più utenti spazialmente diffusi sul territorio. Se così è, la consumazione del reato (art. 615-ter cod. pen. di accesso abusivo) si consuma laddove ha inizio la condotta, ossia il luogo da cui parte il dialogo elettronico tra i sistemi interconnessi e dove le informazioni vengono trattate dall'utente, cioè il luogo di connessione di quest'ultimo».

14) G. Panucci, op cit.: "*Una botnet è una rete di computer, detti bot o zombie, solitamente PC, controllata da un botmaster e composta da dispositivi infettati da malware (ossia da un virus) specializzato (ad es. un trojan), che consente al botmaster di controllarli tutti da remoto in uno stesso momento tramite il proprio dispositivo centrale. In questo modo, tutti i dispositivi infettati diventano parte della botnet e vengono manovrati da remoto dal botmaster. I computer così infettati, possono scagliare attacchi, denominati, Distributed Denial of Service contro altri sistemi e/o compiere altre operazioni illecite; le botnet più famose constavano di ½ milione di dispositivi connessi. Ad esempio, da Anonymous le botnet sono state utilizzate per scagliare attacchi contro i siti istituzionali dello Stato, mediante un accesso congiunto al sito da attaccare di tutti i dispositivi connessi alla botnet per far andare in crash i relativi server, non capaci di sostenere una richiesta di accesso di un numero così elevato di dispositivi e relative connessioni. Si capisce bene che, a fronte di un numero così elevato di condotte (perché poi assume rilevanza ogni singolo accesso eseguito da ogni dispositivo infettato), il criterio della competenza radicato sul posizionamento del server di connessione di ciascuno di essi non avrebbe consentito di individuare un luogo unitario di commissione del reato; laddove invece a ciò si addiviene se utilizziamo l'ultimo criterio elaborato dalla Cassazione, vale a dire quello del luogo di connessione dell'autore del reato, ossia il luogo ove il c.d. botmaster fa partire l'attacco manovrando col suo dispositivo tutti gli altri zombie infettati e che fanno parte della botnet*".

Pertanto, anche la frode informatica si consuma nel momento in cui l'agente consegue l'ingiusto profitto con correlativo danno patrimoniale altrui (giurisprudenza costante, Cass., Sez. I, n. 36359 del 20/05/ 2016, dep. 01/09/ 2016, Rv. 268252; conf. Sez. 2, n. 10354 del 05/02/2020 Ud., dep. 17/03/2020, Rv. 278518, nella cui motivazione la Corte ha precisato che la manipolazione del sistema informatico, in quanto modalità "speciale" e tipizzata di espressione dei comportamenti fraudolenti necessari per integrare la truffa "semplice", non esaurisce e perfeziona l'illecito che, pertanto, si consuma nel momento dell'ottenimento del profitto).

Va segnalata, tuttavia, in senso contrario, Cass., Sez. 3, n. 23798 del 24/05/ 2012, dep. il 15/06/2012, Rv. 253633, per cui, ai fini della determinazione della competenza territoriale, nel reato di frode informatica il momento consumativo va individuato nel luogo di esecuzione dell'attività manipolatoria del sistema di elaborazione dei dati, che può coincidere con il conseguimento del profitto anche non economico (fattispecie nella quale il luogo di commissione del reato è stato individuato nella sede della società gestita dagli imputati, presso la quale si trovavano i server contenenti i dati oggetto di abusivo trattamento).

Quanto al c.d. "*phishing*" (utilizzazione informatica di credenziali altrui indebitamente sottratte a fini fraudolenti), esso integra il reato di frode informatica, come ormai pienamente riconosciuto nella più recente giurisprudenza della Corte di legittimità (Cass., Sez. II, Sentenza n. 9891 del 24/02/2011, depositata 11/03/2011, Rv. 249675; Cass., Sez. I, n. 29692 del 23/06/2010, depositata il 28/07/2010, non massimata; Cass., Sez. II, n. 7764 del 09/02/2010, dep. il 26/02/2010, non massimata; Cass., Sez. I, n. 11506 del 02/02/ 2010, dep. il 25/03/2010, non massimata).

Secondo tale indirizzo, ormai univoco, va affermato il principio che la mera ricezione delle somme provento del *phishing* può ben configurare anche la condotta di ricettazione da ritenere avvenuta nel luogo dove il denaro di provenienza delittuosa è stato ricevuto o accreditato.

Peraltro la più recente giurisprudenza consentirebbe persino di configurare la più grave ipotesi di riciclaggio (Cass., Sez. VI, n. 43534 del 24/04/2012, dep. il 09/11/2012, Rv. 253798; Cass., Sez. II, n. 546 del 07/01/2011, dep. l'11/01/2011, Rv. 249445; Cass., Sez. II, n. 1422 del 14/12/2012, dep. l'11/01/2013, Rv. 254050) da parte di chi mette a disposizione la propria carta prepagata per ostacolare la provenienza delittuosa delle somme da altri ricavate dall'illecito utilizzo di una carta clonata, consentendo il versamento del denaro in precedenza prelevato al bancomat dal possessore di quest'ultima (resosi responsabile del delitto di frode informatica), ovvero consentendo

il diretto trasferimento sulla predetta carta prepagata delle somme ottenute dal possessore della carta clonata, con un'operazione di ricarica presso lo sportello automatico, assumendo rilievo, in tale seconda ipotesi, il delitto presupposto di falsificazione o alterazione della carta originaria di cui all'art. 55, comma 9, d.lgs. n. 231/2007, attualmente previsto dall'art. 493-*ter* cod. pen. Ai fini della competenza il delitto di riciclaggio si è realizzato nel luogo in cui è stata attivata la carta PostePay sulla quale è confluito il denaro provento del reato di frode informatica, univocamente individuabile ex art. 8 cod. proc. pen. quale luogo in cui è stata compiuta parte dell'azione.

Sempre ai fini dell'individuazione della competenza vale, poi, la pena di evidenziare che «*ai fini della configurabilità del reato di cui all'art. 635-quater cod. pen.* (Danneggiamento di informazioni, dati e programmi informatici) *per "sistemi informatici o telematici", oggetto materiale della condotta di danneggiamento, deve intendersi un complesso di dispositivi interconnessi o collegati con unità periferiche o dispositivi esterni (componenti "hardware") mediante l'installazione di un "software" contenente le istruzioni e le procedure che consentono il funzionamento delle apparecchiature e l'esecuzione delle attività per le quali sono state programmate (fattispecie relativa alla distruzione, al fine di perpetrare un furto, di due telecamere esterne dell'area di accesso ad una casa di cura, che la Corte ha riconosciuto come componenti periferiche di un "sistema informatico" di videosorveglianza, in quanto strumenti di ripresa e trasmissione di immagini e dati ad unità centrali per la registrazione e memorizzazione)*» (Sez. 5, n. 4470 del 08/01/2020, dep. 03/02/2020, Rv. 277855). Considerato che tanto il reato di cui all'art. 635-*bis* cod. pen., che i seguenti di cui agli artt. 635-*ter*, 635-*quater*, 635-*quinquies* cod. pen., sono reati di evento, si ritiene che la competenza territoriale si radichi nel luogo in cui si realizza il danno, ancorché la condotta sia delocalizzata.

Il reato di *rivelazione di comunicazioni fraudolentemente intercettate* (art. 617-*quater*, commi 2 e 4, cod. pen. in relazione all'art. 623-*bis* cod. pen.), afferma la giurisprudenza di merito, si consuma nel luogo in cui è diffuso il segnale che rivela al pubblico le immagini abusivamente captate (Trib. Milano 30 ottobre 2002, Ricci, in *Giur. merito*, 2003, 736).

Quanto agli istituti del concorso e della connessione tra reati, ai sensi dell'art. 12 cod. proc. pen., che implicano l'applicazione dei criteri di cui all'art. 16 cod. proc. pen., risulta interessante evidenziare che nel caso di concorso tra le condotte di fraudolenta intercettazione di comunicazioni informatiche e di rivelazione delle comunicazioni, considerato che le fattispecie si consumano, rispettivamente, nel luogo di ricezione e di diffusione del segnale che rivela al pubblico quanto captato, il giudice competente è da individuare

in quello nel cui circondario è situato il luogo di commissione del primo reato, ossia quello del luogo di captazione del segnale.

Da ultimo, il reato di *detenzione di materiale pedopornografico* di cui all'art. 600-*quater* cod. pen., si consuma nel luogo in cui si trova il dispositivo elettronico in cui il detentore conserva il materiale (PC fisso o hard-disk), ma se si tratta di dispositivo mobile (tablet, smartphone, pc portatile) o, a maggior ragione in caso *temporary internet files*, come già osservato, in cui i *files* si trovano allocati in un *server* remoto (cfr. *supra*, nota n. 7) deve farsi riferimento, in assenza di univocità degli elementi acquisiti ai criteri suppletivi di cui all'art. 9 cod. proc. pen. e, primieramente, al luogo in cui è stato effettuato il caricamento o il *download* dei *files*, in seconda battuta al luogo di residenza dell'indagato.

6. La competenza per i "reati occasionalmente in rete". Casistica negli orientamenti della Procura Generale presso la Corte di Cassazione

In maniera dettagliata gli orientamenti della Procura Generale presso la Corte di Cassazione, dopo diversi cambiamenti di rotta attuati dall'Ufficio a partire dal 2008, sono giunti, dopo una consolidata prassi, ad individuare la competenza di alcuni reati più frequenti commessi con il mezzo informatico, che ci si permette di riportare di seguito.

La *truffa on line* (che si ha nel caso in cui la condotta decettiva raggiunge la vittima mediante sistemi informatici, web o piattaforme commerciali) si configura, come la truffa tradizionale, quale delitto istantaneo di danno, che si perfeziona nel luogo del conseguimento dell'effettivo profitto, con il contestuale concreto danno patrimoniale subito dalla parte offesa.

Il criterio discretivo per l'individuazione della competenza territoriale, pertanto, deve essere fondato sulle diverse modalità con le quali la persona offesa abbia effettuato il pagamento.

In ragione della istantaneità/irrevocabilità/irreversibilità ovvero della retrattabilità/revocabilità dell'operazione, rilevano rispettivamente il luogo in cui la persona offesa ha effettuato l'operazione e il luogo in cui l'autore ha conseguito il vantaggio patrimoniale.

La scelta si fonda sul presupposto che l'operazione irrevocabile realizza contestualmente sia l'effettivo conseguimento dell'ingiusto arricchimento da parte dell'agente – che ottiene l'immediata disponibilità della somma versata, e non un mero diritto di credito – sia la definitiva perdita dello stesso bene da parte della vittima.

In applicazione del principio, pertanto, andrà accertato:

1. in caso di pagamento a mezzo vaglia postale ordinario, il luogo ove il vaglia viene materialmente riscosso;

2. in caso di pagamento a mezzo vaglia postale veloce, il luogo in cui la persona offesa ha disposto il pagamento ossia dove ha effettuato il vaglia e non quello in cui l'indagato ha concretamente riscosso il denaro. A differenza dell'ordinario vaglia postale che può essere posto nel nulla, pur in tempi brevi, il vaglia veloce ha come caratteristica che il pagamento del corrispettivo viene effettuato con l'inserimento di una parola chiave indicata dal beneficiario, cui consegue la sua non revocabilità una volta eseguito. In tal senso si è pronunciata Cass. Sez. II, Sentenza n. 14317 del 06/02/2018 Ud. dep. 28/03/2018, Rv. 272515 - 01, secondo cui «il reato di truffa si perfeziona nel momento in cui alla realizzazione della condotta tipica abbiano fatto seguito la "*deminutio patrimonii*" del soggetto passivo e la "*locupletatio*" dell'agente, sicché, qualora l'oggetto materiale del reato sia costituito da "vaglia cambiari veloci", il reato si consuma nel momento e nel luogo in cui viene compiuta l'operazione di disposizione patrimoniale, in ragione delle particolari modalità di negoziazione dei vaglia cambiari veloci (compilazione del modulo con comunicazione della parola chiave necessaria per ottenere il pagamento presso qualunque ufficio postale), per cui una volta realizzata la disposizione il destinatario acquisisce in modo certo il relativo diritto, mentre la successiva monetizzazione è mera modalità esecutiva dell'illecito truffaldino»;

3. in caso di pagamento a mezzo "bonifico ordinario, pagamento on-line o rimessa su conto-corrente", trattandosi di operazione non istantanea e revocabile, il luogo ove ha sede la filiale dell'istituto di credito presso il quale l'autore della condotta ha aperto il conto corrente su cui sono state accreditate le somme tramite bonifico bancario (Cass., Sez. II, Sentenza n. 54948 del 16/11/ 2017, depositata il 07/12/ 2017, Rv. 271761);

4. in caso di pagamento a mezzo di "bonifico urgente", essendo comunque da escludere la contestualità tra il pagamento da parte dell'acquirente e la ricezione da parte del destinatario, il luogo in cui l'agente ha conseguito l'ingiusto profitto;

5. in caso di pagamento a mezzo "bonifico bancario istantaneo" (in inglese *instant payment* ovvero pagamento immediato, che si distingue dal bonifico ordinario per la velocità con cui viene portato a termine il trasferimento di denaro), poiché il trasferimento della somma viene effettuato in tempo reale e la conclusione dell'operazione avviene in pochi secondi (in media 10 cosicché, una volta effettuata la conferma dell'operazione, è impossibile revocare il pagamento), stante il carattere di irreversibilità del mezzo

di pagamento utilizzato, il luogo nel quale la persona offesa ha effettuato il pagamento;

6. tuttavia, nel caso di acquisto di bene posto in vendita su un sito, quale Ebay o simili, previa trattativa con invio delle coordinate bancarie svolta in via telematica (esempio WhatsApp), con bonifico ed accredito della relativa somma su conto corrente on-line "puro", in cui le cui operazioni bancarie possono essere effettuate esclusivamente tramite operazioni telematiche (esempio Conto Arancio acceso tramite una connessione ad Internet presso "Ing Bank", istituto bancario totalmente on-line), va tenuto presente che non può farsi riferimento al circuito Internet come luogo inteso in senso fisico, trattandosi di una realtà virtuale e smaterializzata, per cui non è individuabile il luogo in cui è stato conseguito il profitto, né risulta noto il luogo dove è stata posta in essere una parte dell'azione (art. 9, c. 1, cod. proc. pen.), considerato che l'apparecchio è stato proposto in vendita su sito online e la trattativa è avvenuta in via telematica. In tal caso, per l'individuazione del luogo di consumazione del delitto deve farsi ricorso al criterio suppletivo di cui all'art. 9, c. 2 cod. proc. pen., cioè al luogo di residenza, domicilio o dimora dell'indagato che non coincide con il luogo dove risulta essere stato compilato e firmato il contratto di attivazione del conto. Invero, trattandosi di conto corrente online attivato tramite una connessione ad Internet, non è noto il luogo ove è avvenuto l'accesso da remoto;

7. in caso di "ricarica" di carta di pagamento prepagata (es. PostePay), trattandosi di operazione irrevocabile, il luogo in cui la persona offesa ha proceduto al versamento del denaro sulla carta (es. ricevitoria tanto che ciò avvenga in contanti, quanto con carta di pagamento; da ultimo si veda Cass., Sez. I, n. 3836 del 12/09/2017, dep. il 26/01/2018, Rv. 272291 e Cass., Sez. II, n. 14730 del 10/01/2017, dep. il 24/03/2017, Rv. 269429);

8. in caso di "bonifico bancario ordinario" indirizzato ad una "carta prepagata" dotata di IBAN, che funge anche da conto online (es. PostePay Evolution), non sussistendo un conto materialmente aperto presso una agenzia dell'istituto di credito, il luogo in cui è stata "attivata la carta";

9. Tuttavia, quando l'operazione di pagamento sia avvenuta tramite "postagiro" su carta "Postepay Evolution" dotata di IBAN, con addebito e accredito in pari data, va tenuto presente quanto risulta dal sito ufficiale di Poste Italiane: "Il Postagiro è il modo di trasferire denaro da un conto corrente postale ad un altro. Per eseguirlo, puoi recarti in ufficio postale, oppure accedere al tuo conto BancoPosta tramite il servizio di homebanking. Ti dà la possibilità di effettuare operazioni sia in ambito nazionale che internazionale. Ed è la modalità più veloce ed economica per trasferire denaro in tempo reale

fra correntisti BancoPosta. La transazione effettuata da un ufficio postale non ha limiti di importo, eccetto quelli relativi alla disponibilità del conto. Con Postagiro online puoi trasferire denaro via web in tempo reale a un altro conto corrente BancoPosta…". In particolare, con riferimento all'operazione indirizzata ad una carta Postepay Evolution, che "avendo ad essa associati i codici IBAN BIC e SWIFT, in questo caso risulta del tutto paragonabile ad un Banco Posta. L'operazione è veloce sia nel modo in cui si esegue, sia nell'esito dello spostamento (il trasferimento in condizioni normali impiega meno di un minuto)". Ne consegue che chi dispone il pagamento perde immediatamente la disponibilità del denaro che in tempo reale transita sul conto/carta del destinatario. L'operazione, pertanto, è assimilabile al bonifico istantaneo, cosicché la competenza si radica presso l'Ufficio nel cui Circondario è ricompreso il luogo nel quale la persona offesa ha effettuato il pagamento[15].

Per il reato di *diffamazione via internet* è pacifica in giurisprudenza (Cass., Sez. V, n. 31677 del 19/05/2015, dep. il 21/07/2015, Rv. 264521; Cass., Sez. I, n. 16307 del 15/03/2011, dep. il 26/04/2011, Rv. 249974) l'affermazione secondo cui (tanto con riferimento ai quotidiani online, quanto alle espressioni pubblicate sui social) l'inserimento di frasi offensive o di immagini denigratorie nella rete telematica dà luogo ad un reato di evento che si consuma nel momento e nel luogo in cui i terzi – una persona – percepiscono l'espressione ingiuriosa.

Tuttavia, quando non è noto il luogo in cui le espressioni inserite nella rete telematica sono state percepite da terzi, interviene il criterio suppletivo di cui all'art. 9, comma 1, cod. proc. pen., ovvero il luogo in cui è stata tenuta parte della condotta, che coincide con quello in cui l'agente ha caricato le informazioni diffamatorie sul sito web.

Nel caso in cui non sia noto nemmeno il luogo di inserimento dei dati sul web, si farà ricorso al criterio suppletivo di cui all'art. 9, comma 2 cod. proc. pen., cioè al luogo di residenza, domicilio o dimora dell'indagato, ovvero ancora al criterio suppletivo di cui all'art. 9, comma 3, cod. proc. pen.

Va precisato che il luogo nel quale risultano immesse nel web le espressioni ritenute lesive dell'altrui reputazione viene in considerazione, quale cri-

15) L'eccessiva ampiezza della casistica ha portato qualche autore (A. Nobili - F. Cajani, *Contributo per una riforma normativa in tema di competenza territoriale delle truffe su piattaforma informatica*) ad invocare l'integrazione dell'art. 8 cod. proc. pen. con una disposizione specifica per i reati in rete: «*All'articolo 8 del c.p.p. viene aggiunto il comma 1-bis: "1-bis. Se si tratta di un reato di truffa su piattaforma informatica ed è stato eseguito il pagamento di quanto posto in vendita a mezzo di una carta ricaricabile abbinata ad un conto corrente postale o bancario, è competente il giudice del luogo ove risulta pervenuto il pagamento; ove invece la carta ricaricabile non sia abbinata ad un conto corrente postale o bancario, si applicano i criteri di cui all'art. 9 comma 2 c.p.p."*».

terio di riferimento, qualora manchi l'effettiva percezione della notizia trattandosi di reato tentato.

7. Competenza territoriale dei "reati occasionalmente in rete". Segue casistica in dottrina e giurisprudenza

La dottrina e la giurisprudenza nel tempo si sono occupate dell'individuazione della competenza territoriale per diverse fattispecie realizzate mediante la rete, appuntandosi di volta in volta sulla condotta o sull'evento, ricorrendo, infine ai criteri residuali in caso di incertezza. L'elenco che segue, senza pretesa di esaustività, riguarda ipotesi *pilota*, i cui principi sono utilizzabili per le fattispecie assimilabili.

Per il reato di *distribuzione, divulgazione o pubblicizzazione per via telematica di materiale pedopornografico* (art. 600-*ter*, comma 3, cod. pen.) "*il luogo di consumazione del reato coincide con il luogo nel quale è stato digitato il comando di invio delle foto per via internet. Tale momento corrisponde, infatti, al momento di perfezionamento della fattispecie, ossia all'immissione nella rete del materiale fotografico illecito, a disposizione dei potenziali destinatari*" (Cass. Sez. 3, n. 8296 del 02/12/2004, dep. 03/03/2005, Rv. 231244). In maniera conforme, la Corte di Cassazione si è pronunciata anche di recente: "*Competente a conoscere del reato di pornografia minorile commesso per via telematica è l'ufficio giudiziario nella cui circoscrizione si trova il dispositivo informatico mediante il quale è stato impartito il comando di immissione in rete del materiale pedopornografico*" (Sez. 1, n. 47086 del 17/07/2018 Cc., dep. 16/10/2018, Rv. 274366);

Anche il reato di *violenza sessuale* di cui all'art. 609-*bis* cod. pen., come detto può configurarsi a distanza, infatti, la giurisprudenza di legittimità ha affermato che "*integra il reato di violenza sessuale e non quello di molestie di cui all'art. 660 cod. pen. la condotta di chi, per soddisfare o eccitare il proprio istinto sessuale, mediante comunicazioni telematiche che non comportino contatto fisico con la vittima, induca la stessa al compimento di atti che comunque ne coinvolgano la corporeità sessuale e siano idonei a violarne la libertà personale e non la mera tranquillità. (Fattispecie in cui la Corte ha ritenuto immune da censure la sentenza con la quale il ricorrente era stato condannato per il delitto di violenza sessuale per avere indotto, con plurime comunicazioni telematiche, una minore degli anni 14 a compiere giochi erotici e ad avere rapporti sessuali virtuali)*" (Sez. 3, n. 41951 del 05/07/2019, dep. 11/10/2019, Rv. 277053 - 01).

Con riferimento alla competenza territoriale: "*Ai fini della determinazione della competenza per territorio, va individuato il momento di perfezionamento della fattispecie incriminatrice, facendo riferimento, non solo alla esecuzione della condotta esteriore richiesta per la sussistenza del reato da parte dell'autore, ma, soprattutto, al momento di partecipazione al delitto da parte del minore e, quindi, alla concretizzazione dell'offesa del bene-interesse tutelato: non può dubitarsi, come a giusta ragione argomentato dal giudice di merito, come, nella specie, la partecipazione delle minori, attraverso il compimento di atti di autoerotismo, cui le stesse venivano indotte dal prevenuto, si realizzava nel luogo ove le stesse minori si trovavano nel momento degli incontri via web*" (in motivazione Sez. 3, n. 25822 del 09/05/2013, dep. 12/06/2013, Rv. 257139).

Analogamente, con riferimento alle modalità esecutive tramite *web* «*integra il reato di* sfruttamento della prostituzione (art. 3, legge 20 febbraio 1958, n. 75) *la condotta di chi recluta persone e consente l'effettuazione di prestazioni sessuali a pagamento in videoconferenza via "web-chat", in modo da consentire al fruitore delle stesse di interagire in via diretta ed immediata con chi esegue la prestazione, con la possibilità di richiedere il compimento di determinati atti sessuali. (In motivazione, la Corte ha ribadito che l'attività di prostituzione può consistere anche nel compimento di atti sessuali di qualsiasi natura eseguiti su sé stesso in presenza di colui che, pagando un compenso, ha richiesto una determinata prestazione senza che avvenga alcun contatto fisico fra le parti)*» (Sez. 3, n. 17394 del 09/04/2015, dep. 27/04/2015, Rv. 263358) e anche "*in tema di* prostituzione minorile (art. 600-*bis* cod. pen.)*, rientra nella nozione di prostituzione qualsivoglia attività sessuale posta in essere dietro corrispettivo di denaro, anche se priva del contatto fisico tra i due soggetti, i quali possono anche trovarsi in luogo diverso, essendo unicamente richiesta la possibilità per gli stessi di interagire (fattispecie di prestazione chiesta ed ottenuta via telefono)*" (Sez. 3, n. 7368 del 18/01/2012, dep. 24/02/2012, Rv. 252133); infine, con riferimento al concorso di persone nel reato, si ritiene che le fattispecie siano configurabili anche "*nei confronti di coloro che abbiano reclutato gli esecutori delle prestazioni o che abbiano reso possibile i collegamenti via internet, atteso che l'attività di prostituzione può consistere anche nel compimento di atti sessuali di qualsiasi natura eseguiti su se stesso in presenza di colui che, pagando un compenso, ha richiesto una determinata prestazione al fine di soddisfare la propria libido, senza che avvenga alcun contatto fisico fra le parti*" (Sez. 3, n. 15158 del 21/03/2006, dep. 03/05/2006, Rv. 233929).

Considerato, quindi che le fattispecie comportano la partecipazione del-

la persona la cui prostituzione è oggetto di sfruttamento, e che è possibile che vi siano più fruitori o, comunque, compartecipi, si ritiene che per l'individuazione della competenza territoriale, possa essere applicata la medesima giurisprudenza consolidatasi per la violenza sessuale *online*, e quindi far riferimento al luogo in cui si trova la persona sfruttata.

Le scommesse sull'esito di competizioni sportive gestite da organizzazione avente sede all'estero su avvenimenti sportivi italiani riservati dalla legge al Coni o ad altri concessionari, integrano gli estremi del reato di cui all'art. 4, commi 2 e 3, legge 13 dicembre 1989, n. 401, rispettivamente dando la pubblicità e partecipando al gioco. Nel caso sottoposto all'esame della Corte di Cassazione «*poiché gli scommettitori operavano con la società di allibratori stranieri mediante un rapporto di provvista istituito presso istituto bancario italiano ed attraverso l'utilizzazione del relativo conto corrente essi pagavano le poste e riscuotevano le vincite, attività che si svolgevano in territorio italiano, così come le scommesse vertevano su attività sportive italiane gestite dal C.O.N.I. e in Italia veniva proposta e pubblicizzata l'offerta, doveva applicarsi, conseguentemente, l'art. 6 cod. pen., in considerazione pure del principio della c.d. "territorialità temperata" (posto dal secondo comma di tale norma), secondo il quale un reato si considera commesso in Italia anche se l'azione o l'omissione che lo costituisce è avvenuta solo in parte nel nostro Paese ovvero quivi si è verificato il mero evento che è la conseguenza dell'azione od omissione "contra legem"*» (Sez. 3, n. 519 del 13/02/ 1997, dep. 08/03/1997, Rv. 207288; da ultimo, conf. Sez. 3, n. 25439 del 09/07/2020, dep. 09/09/2020, Rv. 279869).

Per l'integrazione del reato è sufficiente l'impiego di *computers*, *fax* o *modem* (Sez. 3, n. 2947 del 20/09/ 1995, dep. 16/11/1995, Rv. 202786; Sez. 3, n. 2449 del 18/06/1997, dep. 26/09/1997, Rv. 209227) o della rete *Internet* (Sez. 3, n. 36038 dell'08/09/2004, in *Giur. it*., 2005, 1260) quali strumenti per raccogliere e trasmettere le scommesse e le giocate.

L'abusiva duplicazione ed indebita diffusione in rete, in Italia e all'estero, di programmi per elaboratore elettronico (art. 171-*bis*, legge 22 aprile 1941, n. 633) è perseguibile con la legge penale italiana con riferimento agli atti di immissione in rete di informazioni che sono digitate da un terminale che si trovi sul territorio nazionale, ma anche con riferimento alle azioni di riproduzione, memorizzazione o ritrasmissione mediante *server*, sistemi informatici o snodi di rete ubicati in Italia di dati provenienti dall'estero.

8. Riflessioni finali

La materia trattata, proprio perché in continuo divenire, non consente di trarre delle conclusioni ma solo degli auspici, alla luce di alcuni punti di partenza che si ritiene debbano essere tenuti in considerazione ai fini della individuazione del luogo di consumazione del reato ai sensi dell'art. 8 cod. proc. pen.: laddove si verta in ipotesi di reato in rete di mera condotta, il riferimento è quello del luogo in cui l'autore del fatto ha fatto accesso alla rete; laddove si verta in ipotesi di reati di evento, il punto di riferimento da tenere in considerazione è quello del luogo di verificazione del danno; infine, laddove il reato preveda una partecipazione attiva della persona offesa, non si può prescindere dalla considerazione del luogo in cui si trovi quest'ultima.

Una volta che l'utilizzo degli elementi sopra indicati non consenta di superare l'incertezza sull'individuazione del luogo in cui si radica la competenza territoriale, occorre far riferimento ai criteri suppletivi di cui all'art. 9 cod. proc. pen.

Da ultimo, nel corso della discussione seguente alla relazione, è emerso uno spunto assai interessante fornito dai frequentatori: una convinta critica alla iperspecializzazione invalsa nei grandi Uffici di Procura con l'istituzione di gruppi di Sostituti Procuratori dedicati ai reati informatici. Si è correttamente sostenuto che il fenomeno dei reati in rete è ormai fenomeno assai diffuso, e la connessione tra realtà concreta e realtà virtuale è continua e tutti gli operatori debbono essere in grado di intervenire con elevata professionalità.

Si osserva che corrisponde a quotidianità la necessità di intervenire su reati, anche comuni, commessi con il mezzo informatico, pertanto, tutti i componenti degli Uffici di Procura ed anche della polizia giudiziaria debbono essere alfabetizzati in tal senso ed intervenire tempestivamente e con competenza. Purtuttavia proprio l'esistenza della disposizione di cui all'art. 51, comma 3-*quinquies*, cod. proc. pen., che attribuisce alle Procure distrettuali e l'art. 328, comma 1-*quater*, cod. proc. pen., che attribuisce al G.I.P./G.U.P. distrettuale la competenza per i reati in esso enumerati, impongono una specifica specializzazione nell'intervento, che risulta assai opportuna, ma che deve costituire un *quid pluris* rispetto alla conoscenza della rete e di tutte le ipotesi, sempre più raffinate e diffuse di cui tutti gli operatori del diritto debbono avere cognizione.

Bibliografia

Allieri I.M., Consigliere della Corte d'Appello di Ancona, già referente per il settore penale della Struttura didattica della Corte d'Appello di L'Aquila, *Brevi note introduttive*, SSM Struttura didattica territoriale C.A. L'Aquila "I reati commessi con l'uso dei sistemi informatici e telematici", Tribunale di Pescara, 24 giugno 2016

Cajani F., Sostituto Procuratore alla Procura della Repubblica di Milano, e Cavallo F., *Le truffe su piattaforma di e-commerce: l'esperienza della procura di Milano*, in "IISFA Memberbook 2015 Digital Forensics. Condivisione della conoscenza tra i membri dell'IISFA Italian Chapter", a cura di Gerardo Costabile - Antonino Attanasio - Mario Ianulardo

Cuomo L., Sostituto Procuratore Generale alla Procura Generale presso la Corte di Cassazione, *I reati commessi in rete: le principali fattispecie e i nuovi problemi interpretativi*, SSM "Il diritto penale del web", Villa di Castel Pulci (Scandicci), 30 maggio 2013

Di Noia F., *Truffe online e competenza territoriale: quando un intervento del legislatore diventa imprescindibile*, capitolo I, in "IISFA Memberbook 2018 Digital Forensics. Condivisione della conoscenza tra i membri dell'IISFA Italian Chapter", a cura di Gerardo Costabile - Antonino Attanasio - Mario Ianulardo

Nobili A. - Cajani F., Sostituti Procuratori alla Procura della Repubblica di Milano, *Contributo per una riforma normativa in tema di competenza territoriale delle truffe su piattaforma informatica*, capitolo II, in "IISFA Memberbook 2018 Digital Forensics. Condivisione della conoscenza tra i membri dell'IISFA Italian Chapter", a cura di Gerardo Costabile - Antonino Attanasio - Mario Ianulardo

Panucci G., Sostituto Procuratore alla Procura della Repubblica di Terni, *Reati informatici e mezzi di ricerca della prova*, SSM Struttura didattica decentrata della C.A. di Catanzaro "Criminalità informatica e tecniche di investigazione", Tribunale di Cosenza, 15.12.2021

Specchio G., Ten. CC Ph.D., *Analisi di contesto del cyberspace*, Scuola Superiore della Magistratura (SSM), struttura didattica decentrata della Corte d'Appello di Roma, "Le condotte ingannevoli nel sistema del diritto penale", Roma, 19 settembre 2019

Le investigazioni mediante strumenti informatici e le prove informatiche

di Carlo Scalas*

1. Introduzione

La tecnologia e Internet hanno comportato la nascita di nuove forme di criminalità (*cyber crimes*) ma anche offerto *ulteriori strumenti per realizzare reati "classici"*. Il vantaggio che offre la rete non è solo la riduzione delle distanze fisiche ma, soprattutto, l'anonimato.

Le odierne tecniche di indagine non vedono la sostituzione degli strumenti informatici alle attività tradizionali, ma un loro affiancamento.

Dal momento che spesso la tecnologia comporta costi economici e di tempo, ogni scelta andrà calibrata sul modello di condotta illecita da affrontare, sul funzionamento del sistema informatico di volta in volta utilizzato, ma anche in relazione ai ristretti termini di conservazione dei dati di traffico, a quelli di durata delle indagini preliminari e al fatto che una richiesta di proroga di questi ultimi ordinariamente comporta un disvelamento del procedimento.

Per queste ragioni, è opportuno da subito svolgere – o richiedere all'Autorità Giudiziaria che vengano svolte – delle preliminari attività che consentano di rendere fruttuosa l'indagine. Molte scelte spettano al P.M., ma questi deciderà anche in base a proposte investigative formalizzate nelle informative o emerse in riunioni di coordinamento con la polizia giudiziaria.

Per concludere questa premessa, va sottolineata l'importanza che riveste la ricostruzione di un'eventuale serialità in questo tipo di indagini.

Spesso si assiste a condotte "polverizzate" che, isolatamente considerate, si connotano per danni patrimoniali di modesto importo. Ricostruire il complessivo agire di un soggetto, tuttavia, è utile a comprenderne non solo la gravità. L'emersione di una catena di reati, invero, permette di disporre di una maggior quantità di materiale probatorio da confrontare e far esprimere sinergicamente alla ricerca della compiuta identificazione del responsabile.

2. Gli indirizzi IP

Il primo passo per individuare il soggetto che ha utilizzato un disposi-

(*) Sostituto Procuratore della Repubblica presso il Tribunale di Milano, Referente Distrettuale per l'Innovazione per il Distretto di Corte di Appello di Milano, Dottore di ricerca in Diritto dei contratti.

tivo in rete consiste nell'acquisire il relativo indirizzo IP (Internet *Protocol*), che identifica univocamente una specifica macchina all'interno della rete.

L'IPv4 è quello generalmente utilizzato ed è costituito da una serie di 4 numeri decimali che vanno da 0 a 255, separati da un punto (es: 68.57.115.25). Digitando su un *browser* la stringa di ricerca "IP *finder*" si raggiungono siti gratuiti che consentono di geo-localizzare un determinato IP.

Ma esistono delle eccezioni alla univocità che possono complicare gli accertamenti. Per avere un risultato maggiormente attendibile, come si vedrà, sarà necessario indicare nella proposta operativa non soltanto il giorno ma anche le ore, i minuti e i secondi dell'accesso di interesse investigativo.

Per meglio comprendere la portata del discorso, è bene considerare che gli IP si distinguono in:

– *pubblici/privati*: quelli pubblici vengono assegnati a un soggetto che poi li concede gerarchicamente a terzi e, quindi, sono veramente univoci. Quelli privati (LAN) si rilevano solo quando si affacciano sulla rete, ma non danno univocità perché potrebbero essere detenuti da più organizzazioni contemporaneamente;

– *statici/dinamici*: talune macchine si vedono assegnato in maniera permanente un IP, mentre ad altre ne viene concesso uno a ogni ingresso in Internet.

A rendere più complessa l'identificazione di un dispositivo in rete, poi, contribuiscono anche:

– *reti NAT (Network Address Translation)*: che permettono ai dispositivi con IP privato di comunicare su Internet sostituendo l'IP privato con uno pubblico. In questo caso, risalire all'IP pubblico non è sufficiente perché potrebbe essere in uso a centinaia di utenti. Occorre sviluppare le informazioni aggiuntive contenute nelle intestazioni dei messaggi (c.d. "*header*") per consentire l'identificazione;

– *reti wireless aperte*: che offrono una schermatura per chi vuole collegarsi da reti non protette o pubbliche;

– *reti proxy*: i *proxy* anonimizzatori sono dei servizi che consentono di camuffare il proprio IP, perché solo il gestore del *proxy* ha le informazioni per risalire al codice identificativo del dispositivo ma spesso è collocato in Paesi esteri poco collaborativi. I sistemi *proxy chain*, poi, si caratterizzano per schermare l'IP attraverso la ripetizione dell'anonimizzazione[1].

1) TOR, ad esempio, consente anche di scegliere i "nodi" attraverso i quali passeranno i propri dati, offrendo serie possibilità di risultare irreperibili, specialmente se si sceglie di far passare la connessione in Paesi con legislazioni permissive.

3. La recente normativa in materia di acquisizione di *file di log* e i termini di *data retention*

A fronte dell'importanza degli indirizzi IP, è necessario chiarire come ottenerli.

L'art. 132 d.lgs. n. 196/03, di recente ritoccato in adeguamento agli spunti comunitari (cfr. CGUE 2.3.2021, causa C-746/18), oggi dispone che il P.M. chieda al GIP l'autorizzazione ad acquisire i dati di traffico telefonico e telematico.

Questi ultimi, altrimenti detti *file di log*, non sono altro che gli IP di connessione.

La novella non ha inciso solo sul procedimento ma anche sul catalogo di reati per i quali è ammessa l'acquisizione, dal momento che oggi si richiede come regola generale che si stia indagando per reati puniti con il massimo edittale non inferiore a 3 anni di reclusione e in relazione ai quali sussistano sufficienti indizi[2].

La normativa interna sommariamente riassunta non risolve tutti i problemi in materia.

Con grande frequenza, infatti, gli *Internet Service Provider* (ISP) che detengono i dati sono allocati all'estero, ove i termini di conservazione sono più ristretti. Per questa ragione occorre inoltrare contestualmente delle richieste di *freezing* tramite il CNAIPIC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture) di Roma, per evitare che *medio tempore* i dati oggetto della richiesta vengano cancellati.

Per individuare gli indirizzi e-mail a cui scrivere messi a disposizione dai maggiori ISP, è sufficiente registrarsi sul sito di EUROPOL, ove si possono scaricare tali informazioni (*guidelines*).

In una recente indagine il CNAIPIC ha fornito supporto per ottenere il *flagging*[3] di alcuni *account* di posta elettronica del *provider* svizzero PROTONMAIL, permettendo di inoltrare fruttuosamente una richiesta di rogatoria. Questo caso concreto offre un esempio dell'importanza di mappare il sistema informatico che diviene di specifico interesse a fini investigativi. Poiché PROTONMAIL offre a pagamento il servizio di attivazione di più *account*, nella rogatoria è stata inserita anche una parte diretta ad acquisire i dati

2) La norma è di interesse anche per i termini di conservazione dei dati, imposti ai *provider* italiani (due anni per il traffico telefonico e 1 anno per quello telematico (*non content*). Tutti i termini, peraltro, sono uniformati a 72 mesi (6 anni) per i reati di cui al 407 comma II lett. a) e 51 comma III *quater* c.p.p. (delitti con finalità di terrorismo) dall'art. 24, comma I, l. n. 167/17.

3) In questo caso, dal momento che l'ISP per *policy* interna non registrava i dati, preliminarmente – ancora prima del congelamento – è stato necessario richiedere che venissero salvati.

relativi allo strumento di pagamento utilizzato, al fine di ottenere più elementi da incrociare tra loro.

Riprendendo il filo della trattazione, va dato atto del fatto che *i principali ISP vedono i propri server allocati negli U.S.A.*

Agli U.S.A. è possibile chiedere senza rogatoria solo dati *non content*, vale a dire i metadati a contenuto non comunicativo (*subscriber information*, cioè i dati forniti al momento della registrazione e i *traffic data*, cioè gli IP). I dati di rilievo contenutistico, per contro, vengono rilasciati solo tramite procedure di urgenza, secondo le *policy* dell'ISP.

4. Le intercettazioni e il *trojan*

Merita qualche cenno anche l'attività tecnica, sebbene non si tratti di uno strumento di recente introduzione e che difficilmente risulta proficuo nella tradizionale declinazione rappresentata dalle intercettazioni telefoniche.

Al di là dell'ampia risonanza mediatica che hanno avuto diverse indagini risolte grazie a questo mezzo di ricerca della prova, va preso atto che sono diverse le applicazioni – quali *Skype*, *Whatsapp*, ecc. – che consentono di intraprendere una conversazione vocale di fatto non intercettabile o, comunque, di scambiarsi messaggi di testo o audio. A fronte dell'attuale panorama tecnologico e del *diverso atteggiarsi delle interazioni sociali, diventa fondamentale la preliminare attività di studio delle abitudini dei bersagli* per meglio comprendere quali tecniche di indagine possono avere successo. In taluni casi, ad esempio, sarà più proficuo acquisire il contenuto di un dispositivo elettronico attraverso la sua copia forense, mentre in altri potrebbero risultare determinanti delle intercettazioni tra presenti attraverso una microspia ben collocata.

Le attività captative – siano esse telefoniche, ambientali o telematiche – sono ammesse in presenza di gravi indizi dei reati di cui all'art. 266 c.p.p.

La serialità, ancora una volta, può venire in soccorso non soltanto per comprendere come e dove intercettare, ma anche per ricostruire eventuali ipotesi associative. Laddove si accerti il cooperare di almeno tre persone, invero, sarà possibile contestare la fattispecie di cui all'art. 416 c.p. finalizzata alla commissione anche di reati che – isolatamente considerati – non consentirebbero l'impiego di questo strumento investigativo.

Sul punto, inoltre, va rammentato che la giurisprudenza si è consolidata ormai nel ravvisare l'associazione per delinquere anche al di fuori delle ipotesi tradizionali (come quelle finalizzate alle rapine o al traffico di stu-

pefacenti), sempre che ricorrano degli elementi sintomatici che denotino la sussistenza di un vincolo tra i correi, che sopravvive al singolo reato[4]. I reati associativi, peraltro, permettono di intercettare nei luoghi di privata dimora anche in assenza del tradizionale requisito rappresentato dal fondato motivo di ritenere che ivi si stia svolgendo attività criminosa[5].

Un'ipotesi alla quale talvolta non si pensa per ottenere intercettazioni nel domicilio al di fuori delle ipotesi di criminalità organizzata è quella del *possesso di beni come armi o stupefacenti*, che di per sé integra una fattispecie di reato che le consentirebbe.

Come è noto, ai sensi dell'art. 1140 comma II c.c. "*si può possedere direttamente o per mezzo di altra persona, che ha la detenzione della cosa*". Tale norma rappresenta il fondamento del principio in forza del quale il possesso può essere conservato anche *solo animo*, purché il possessore abbia la possibilità di ripristinare il contatto materiale con la cosa quando lo voglia.

Al riguardo, la Suprema Corte di Cassazione ha chiarito che «*il possesso (o la detenzione) può essere conservato "solo animo", purché il possessore (o il detentore) sia in grado di ripristinare "ad libitum" il contatto materiale con la cosa, sicché, ove tale possibilità sia di fatto preclusa da altri o da una obiettiva mutata situazione dei luoghi, l'elemento intenzionale non è, da solo, sufficiente per la conservazione del possesso (o della detenzione), che si perde nel momento stesso in cui è venuta meno l'effettiva disponibilità della cosa*» (cfr. Cass. civ. n. 1723/16).

Ragionando in questi termini, allora, sarà possibile richiedere un'ambientale all'interno del domicilio di un indiziato di omicidio commesso per il tramite di un'arma da sparo, laddove si riesca a sostenere che tale soggetto ragionevolmente terrà a portata di mano l'arma utilizzata per proteggersi dalle possibili ritorsioni dei parenti o dei complici della persona offesa deceduta.

Venendo al *captatore informatico* (c.d. *trojan*), proprio i limiti alle intercettazioni nei luoghi qualificabili come domicilio hanno rappresentato la ragione sottesa all'orientamento restrittivo della Suprema Corte di Cassazio-

4) In questo senso, si è affermata la sussistenza di una compagine criminale anche in presenza di reati contro la pubblica amministrazione (corruzione e turbativa d'asta), in presenza di indici sintomatici quali la serialità, il reiterare condotte con modalità sovrapponibili, il sensibile periodo temporale, l'ingente profitto economico e l'agire sinergico dei compartecipi (cfr. Cass. n. 15573/17).

5) La disciplina di favore di cui all'art. 13 d.l. n. 152/91, come è noto, permette l'intercettazione in deroga ai presupposti ordinari quando essa appare semplicemente "*necessaria*" (e non indispensabile), in presenza di "*sufficienti*" (e non gravi) indizi di reato, per una durata iniziale di 40 giorni e di 20 giorni per ogni proroga (e non di 15+15), nonché "*per lo svolgimento delle indagini*" (e non per la prosecuzione, vale a dire anche come primo atto di indagine).

ne, chiamata a pronunziarsi sulla legittimità del suo utilizzo quando ancora il Legislatore non lo aveva disciplinato.

La peculiarità del *trojan*, invero, è data dal fatto di dar vita a una captazione "itinerante", dal momento che l'inserimento di uno *spyware* all'interno di un dispositivo mobile che viene costantemente portato con sé dal soggetto che si intende intercettare, comporta il rischio di registrare conversazioni anche all'interno dei relativi luoghi di privata dimora. La sentenza delle Sezioni Unite n. 26889/2016 imp. Scurato, quindi, ne aveva circoscritto l'uso alle sole ipotesi di criminalità organizzata, nelle quali è sempre possibile l'intercettazione anche in luoghi di privata dimora ai sensi dell'art. 13 d.l. n. 152/91. In tal modo, si risolveva a monte il problema delle intercettazioni ambientali in luoghi di privata dimora, non ammettendole se non quando non è richiesto che ivi si stia svolgendo attività criminosa.

Oggi il codice di rito consente il captatore informatico in tutti i casi in cui è possibile un'intercettazione tra presenti, di fatto inquadrandolo come una modalità esecutiva di quest'ultima (art. 266 comma II c.p.p.).

Ma se i reati per i quali si procede non sono di criminalità organizzata o dei pubblici ufficiali e incaricati di pubblico servizio contro la P.A. puniti con pena non inferiore nel massimo a 5 anni, occorre indicare anche i luoghi e il tempo in relazione ai quali è consentita l'attivazione del microfono, "*anche indirettamente determinati*" (art. 267 comma I c.p.p.).

5. Il principio di proporzionalità nelle acquisizioni di copie forensi

Il principio di proporzionalità, di matrice comunitaria, impone di limitarsi al necessario e determina la "giusta misura del potere".

In altri termini, anche il potere giudiziario – nella sua declinazione investigativa – deve essere ragionevolmente ponderato, nel senso che il privato deve subire una limitazione tollerabile e adeguata. Al giorno d'oggi, all'interno di uno *smartphone* si trovano una pluralità di dati sensibili che possono risultare del tutto irrilevanti ai fini investigativi (quali le fotografie ritraenti la vita privata, la rubrica telefonica o la *password* dell'*home banking*) ma che al momento della *discovery* possono finire nelle mani di chiunque abbia accesso al fascicolo.

È principio ormai consolidato[6] quello in forza del quale occorre *contemperare le finalità di indagine e le esigenze di proporzionalità*, in special modo

6) Cfr. Cass. n. 13165/20 e Cass. n. 9989/18.

quando si ha a che fare con soggetti estranei al reato o portatori di interessi qualificati alla riservatezza (quali i giornalisti o i politici). In altri termini, è necessario che vi sia una proporzione tra il mezzo adoperato e l'obiettivo da raggiungere, per evitare annullamenti del vincolo reale apposto sui dispositivi di terzi per ragioni probatorie.

Dal momento che l'art. 42 comma II Cost. pone i limiti alla proprietà privata come un'eccezione alla regola della sua tutela, appare opportuno far ricorso ad *alcuni accorgimenti* per rispettare le coordinate sopra tratteggiate.

In questo senso, nel motivare la richiesta di acquisizione di un dispositivo sarà necessario:

– chiarire specificamente l'aderenza con il fatto che si sta indagando e perché potrebbe essere d'aiuto nelle investigazioni;

– limitare temporalmente il periodo di interesse dei dati che si estrarranno;

– limitare a determinati soggetti le chat che si intenderà copiare;

– anticipare, ove possibile, il sequestro del dispositivo con un'ispezione dello stesso alla ricerca di eventuali elementi di interesse investigativo, sollecitando la collaborazione del soggetto che ne ha la disponibilità.

La *richiesta di consegna* (art. 248 c.p.p.) è un buon strumento per assicurare le finalità probatorie contemperando la proporzione e, peraltro, consente di evitare i riesami.

La richiesta di consegna di una *res* determinata, invero, viene ritenuta dalla giurisprudenza una misura temporanea a scopo conoscitivo priva di finalità ablative, con la conseguenza che – mancando un contenuto autoritativo – il rimedio del riesame non risulta esperibile. La Suprema Corte ha precisato che l'istanza di riesame "*tesa com'è alla revoca di un atto di autorità che spiega sulla situazione giuridica del destinatario immediati effetti ai quali questi deve necessariamente soggiacere, riguarda esclusivamente il decreto di sequestro e non è ammissibile – anche per la tassatività dei mezzi di impugnazione ex art. 568 comma primo cod. proc. pen. – nei confronti del decreto di esibizione di cui all'art. 256 stesso codice, i cui effetti scaturiscono dal volontario, anche se doveroso, adempimento di un obbligo disposto dalla legge (nell'affermare il principio di cui in massima la Cassazione ha altresì evidenziato che il carattere distintivo del sequestro da ogni altra acquisizione, di documenti o cose, al processo non va ricercato nell'effetto pratico, sostanzialmente analogo, ma nella sua natura di atto autoritativo esplicato nell'esercizio di un potere-dovere rispetto al quale corrisponde una posizione di mera soggezione del destinatario)*" (cfr. Cass. n. 3521/91).

A conferma di questa impostazione, anche più di recente la Suprema

Corte ha parlato – con riferimento alla richiesta di consegna – di "sequestro consensuale" (cfr. Cass. n. 13484/2000), vale a dire di provvedimento che non si connota per un tenore autoritativo.

6. La copia forense

Per *Mobile Forensic* si intende l'attività di acquisizione di dati da un dispositivo mobile e dai suoi media associati (schede SIM o SD).

Il codice di rito impone che gli accertamenti e i rilievi urgenti di p.g. (art. 354 c.p.p.), le ispezioni (art. 244 c.p.p.) e le perquisizioni (art. 247 c.p.p.) di sistemi informatici avvengano con procedure che garantiscano:

- la *conservazione dei dati originali*;
- che la *copia sia conforme* all'originale.

Anche il sequestro di dati presso i fornitori di servizi informatici o telematici (art. 254-*bis* c.p.p.) deve essere compiuto con tecniche che garantiscano la conformità delle copie agli originali e l'immodificabilità di questi ultimi.

Per acquisire la copia di un sito *web*, mantenendo fede ai sopra ricordati requisiti, è possibile seguire alternativamente due differenti strade:

- l'uso di un apposito programma di *mirroring* che garantisca le due caratteristiche di cui sopra (come Spiderzilla o HTTrack);
- una registrazione video.

Un tema attuale, sul quale non si è formato ancora un orientamento univoco, attiene al carattere ripetibile o meno dell'attività di copia dei dati contenuti all'interno di un dispositivo. In altri termini, occorre chiedersi se *l'estrazione del contenuto di un dispositivo informatico dà luogo a un'attività di carattere ripetibile o irripetibile*. Se è vero che dare avviso ai difensori neutralizza possibili eccezioni dibattimentali, occorre fare i conti con quei procedimenti nei quali una *discovery* anticipata precluderebbe ulteriori attività a sorpresa.

Una soluzione potrebbe essere mutuata dalla giurisprudenza in materia di rilievi dattiloscopici.

In buona sostanza, ancora prima di ragionare in merito alla ripetibilità della procedura, occorre chiedersi se una simile attività debba qualificarsi come accertamento o mero rilievo. Come è noto, la distinzione risiede nella circostanza che i rilievi non richiedono per l'operatore una spendita di discrezionalità tecnica. Con la conseguenza che, a prescindere da chi li ponga in essere, il loro risultato sarà sempre identico.

In senso contrario, gli accertamenti investono una quota di apprezzamento che varia a seconda della sensibilità e della formazione del tecnico. Per tale ragione, dunque, il codice di procedura distingue tra quelli ripetibili (art. 359 c.p.p.) e quelli irripetibili (art. 360 c.p.p.), ai quali vengono accordati una serie di garanzie.

Pervenendo alla conclusione che si verte nell'ambito dei rilievi, un recente arresto ha statuito che «*non rientra nel novero degli atti irripetibili l'attività di estrazione di copia di "files" archiviati in un computer, trattandosi di un'operazione meramente meccanica e sempre riproducibile, priva di carattere valutativo e che non determina alcuna alterazione dello stato delle cose in grado di pregiudicare la genuinità del suo contributo conoscitivo*» (cfr. Cass. n. 5283/21).

7. Furti di identità e metodi di indagine

La tecnologia e la rete Internet consentono di celare il proprio agire – agevolmente e senza particolari costi – dietro false identità.

Gli *account* di posta elettronica, l'intestazione delle schede telefoniche o dei conti correnti e delle carte di pagamento sovente non forniscono indicazioni univoche in merito al loro effettivo titolare. È sempre più frequente, invero, il fenomeno dei *furti di identità o della creazione di falsi profili*, anche grazie alla collaborazione di soggetti che si trovano in difficoltà economica e che per pochi euro si disinteressano dell'utilizzo che di questi strumenti potrebbe fare chi intende delinquere.

Per addivenire all'individuazione del reale utilizzatore non esiste un unico modo.

In primo luogo, è consigliabile cercare di *comprendere come funziona il sistema impiegato* di volta in volta per delinquere, al fine di individuare cosa occorre per risalire all'identificazione del reo. Si tratta di un tema che diventa fondamentale, in quanto consente di attuare scelte investigative efficaci. Non bisogna dimenticare, invero, che spesso i dati che si intende ricercare sono custoditi in sistemi informatici allocati presso Paesi stranieri, con la conseguenza che simili attività di ricerca e acquisizione richiedono tempistiche dilatate che mal si conciliano con i ristretti termini di indagine prescritti dal nostro codice di procedura.

Per cercare di aggirare la via delle richieste rogatoriali o degli OEI, quindi, sarà opportuno ripiegare su accertamenti collaterali che nella pratica si rivelano efficaci.

Si tratta, a titolo esemplificativo, di verifiche quali:

– l'acquisizione di cartellini anagrafici, al fine di comprendere se i documenti di identità utilizzati sono stati oggetto di contraffazione;

– l'analisi dei bonifici in uscita relativi al conto corrente beneficiario di un pagamento indebito, alla ricerca di acquisti "individualizzanti"[7];

– l'incrocio di dati (ad esempio, tra quelli relativi alla e-mail necessaria per registrarsi a un sito e quelli della carta utilizzata per effettuare pagamenti);

– l'assunzione a s.i.t. del titolare della carta utilizzata per pagare un servizio;

– la verifica del luogo nel quale viene costantemente ricaricata un'utenza telefonica, per acquisire le registrazioni dell'esercizio commerciale;

– l'individuazione dell'indirizzo di spedizione della carta di pagamento o della merce oggetto di condotte truffaldine;

– l'incrocio dei dati riguardanti schede SIM e IMEI identificativi dei telefoni cellulari, allo scopo di individuare ulteriori utenze da intercettare.

La delega di uno o più di questi accertamenti può rappresentare un valido surrogato all'acquisizione di dati da sistemi informatici e permette di rimanere all'interno dei confini nazionali, con indubbio risparmio in termini di tempo.

8. Altri strumenti investigativi atipici

Rimane da trattare il tema relativo ai mezzi di ricerca della prova non espressamente previsti dal Legislatore, che per la loro capacità di incidere sulle libertà fondamentali della persona richiedono particolare attenzione.

A tal proposito, il punto cardinale è rappresentato dal fatto che spesso la legge sottopone la limitazione di tali diritti a particolari cautele. Gli articoli 13, 14 e 15 Cost., ad esempio, prevedono libertà personali comprimibili solo con atto motivato dell'Autorità Giudiziaria e in attuazione di specifiche previsioni normative (c.d. *doppia riserva di legge e giurisdizione*).

Un primo esempio di attività investigativa atipica è rappresentato dall'*agente attrezzato per il suono*.

Nella pratica è stata ritenuta legittimamente acquisibile a dibattimento la registrazione effettuata da un privato grazie a un microfono fornitogli dalla polizia giudiziaria. A tal proposito, è opportuno chiarire che non si tratta di un'operazione assimilabile all'intercettazione di conversazioni secondo i cri-

7) L'esperienza concreta ha restituito acquisti per beni mobili registrati, pagamenti per ristrutturazioni di immobili e acquisti di biglietti numerati per partite di calcio.

teri enunciati dalle Sezioni Unite imp. Torcasio[8], poiché in questi casi la registrazione è effettuata da uno dei due interlocutori (con il microfono indossato) e non da un terzo. Proseguendo in negativo, va chiarito che il risultato della captazione non è classificabile nemmeno come documento ai sensi dell'art. 234 c.p.p.

Come è noto, infatti, è tale solo l'atto che non nasce all'interno del procedimento, mentre in tale ultimo caso ci si trova al cospetto di un atto del procedimento oggetto di documentazione. Per questa ragione, il microfono dovrà essere indossato dal privato e non dalla polizia giudiziaria, in quanto per quest'ultima opererebbero altre norme che dettano inutilizzabilità come l'art. 195 comma IV c.p.p. o l'art. 63 c.p.p.

Sgombrato il campo dal fatto che l'agente "attrezzato" potrà essere solo un privato, la giurisprudenza ha precisato che è necessaria l'autorizzazione del P.M. tramite decreto motivato.

Un ulteriore mezzo di ricerca della prova non disciplinato è costituito dalle *videoriprese senza sonoro*[9].

Al riguardo, si deve sottolineare che per le riprese in un luogo pubblico non occorre alcuna autorizzazione. In questi casi, peraltro, si rientra nella prova atipica prevista dall'art. 189 c.p.p., che verrà assunta ove idonea ad assicurare l'accertamento dei fatti.

I problemi si pongono, per contro, qualora la telecamera venga collocata all'interno di un luogo di privata dimora o ad aspettativa di riservatezza. A fronte della doppia riserva di legge e di giurisdizione che assiste l'inviolabilità del domicilio (art. 14 Cost), nei luoghi di privata dimora la captazione di comportamenti comunicativi è soggetta al regime delle intercettazioni, mentre i comportamenti non comunicativi non possono essere videoregistrati.

In tal senso, invero, si è detto che in mancanza di una specifica disposizione la copertura legale non può certo rinvenirsi nel dettato dell'art. 189 c.p.p.

Tale norma, nel disciplinare l'assunzione delle prove non previste dalla legge, presuppone la loro legittimità.

Con la conseguenza che, in mancanza di una specifica disposizione di legge in questo senso, non sarà sufficiente il provvedimento dell'Autorità Giudiziaria che assolverebbe al solo requisito della riserva di giurisdizione.

---

8) Cfr. Cass. n. 36747/03, secondo la quale per aversi intercettazione occorre: 1) la captazione occulta e contestuale di una conversazione, 2) attuata da soggetto estraneo alla conversazione, 3) con strumenti tecnici.

9) In caso di video assistito da una traccia audio, ovviamente, si rientrerebbe nella disciplina delle intercettazioni tra presenti.

Cybercrime e cooperazione giudiziaria. Il Secondo Protocollo addizionale alla Convenzione di Budapest

di Alberto Cappellini*

Nella lotta al *cybercrime* la cooperazione giudiziaria sul piano internazionale riveste un ruolo di capitale importanza.

La dimensione di confinamento al singolo apparecchio dell'attività informatica, tipica degli albori dell'era digitale, si è infatti ormai da lungo tempo trasformata in un interscambio continuo di informazioni e comandi tra differenti dispositivi, immersi in un ambiente *cyber*, in *internet*.

Così, la fenomenologia del *cybercrime* – comprendente sia reati informatici in senso stretto, sia comunque commessi attraverso l'utilizzo di strumenti informatici, comunque nell'ambiente di *internet* – è andata sempre più assumendo un carattere *smaterializzato*, *ubiquo* e in larga misura *istantaneo*. I confini nazionali, nell'ambiente di *internet*, rivestono un ruolo di sostanziale irrilevanza, potendo le varie singole azioni perpetrare i loro effetti, in modo immediato, praticamente ovunque nel globo.

A fronte dell'enorme impatto della criminalità informatica sulle infrastrutture digitali pubbliche e private la risposta giudiziaria trova grandi difficoltà ad affermarsi. Criminologicamente parlando, la "cifra oscura" del *cybercrime* è elevatissima: molti reati neanche vengono denunciati, e la gran parte delle segnalazioni si traducono in fascicoli di indagine contro ignoti, che non riescono a pervenire al vaglio del dibattimento per la difficoltà nel reperire elementi di prova e nell'identificare i responsabili. La giurisprudenza di merito e di legittimità è scarna, e riguardante perlopiù casistiche (ad esempio, abuso di credenziali) in realtà non propriamente afferenti alla fenomenologia prototipica del *cybercrime*, peraltro anche la più pericolosa: l'*hacking* e il *cracking* da remoto, ovvero la propagazione di *malware* di vario tipo attraverso la rete (si pensi in particolare ai sempre più diffusi *ransomware*).

La risposta giurisdizionale a tali fenomeni, anche quando possa positivamente affermarsi la giurisdizione nazionale rispetto a simili reati, è infatti pesantemente vulnerata dalla facilità con cui l'agire criminoso supera quelle barriere che delimitano le aree di competenza dei singoli Stati; le quali costituiscono invece un argine non direttamente valicabile nell'esercizio dei poteri inquirenti, anche a carattere coercitivo, in assenza di collaborazione da parte dell'autorità giurisdizionale straniera.

(*) Giudice presso il Tribunale di Spoleto; Dottore di ricerca in discipline penalistiche, Università di Firenze.

È dunque, anzitutto, il carattere intrinsecamente transnazionale del *cybercrime* a investire la cooperazione internazionale in campo giudiziario della centralità nella prassi di cui si diceva. Parallelamente, è il carattere sostanzialmente istantaneo di tale criminalità ad aver determinato e, ancora oggi, a determinare la traiettoria evolutiva degli strumenti di cooperazione utilizzabili, alla continua ricerca di modelli più certi nel risultato, semplici e agili, ma soprattutto più rapidi, tali da consentire quantomeno di tentare di "inseguire" una realtà criminale tanto veloce.

Ad oggi non esistono ancora regole sovranazionali unificate di cooperazione in materia di *cybercrime* fra tutti gli Stati, tali da fissare comuni criteri giuridici e protocolli tecnici.

A livello di Nazioni Unite, con la Risoluzione dell'Assemblea Generale 74/247 è stata istituita una Commissione *ad hoc*, in seno all'UNODC, per la preparazione di un progetto di convenzione universale in materia di *cybercrime* da sottoporre all'assemblea stessa, lavori che sono tuttavia attualmente in corso. È un panorama certamente interessante da monitorare, ma al momento privo di effettività sul piano pratico.

Esistono invece importantissimi strumenti di matrice eurounitaria e del Consiglio d'Europa, su cui ci soffermeremo più oltre; nonché, va detto, numerosi altri accordi, soprattutto bilaterali, di assistenza giudiziaria, applicabili (anche) al settore in discussione, rispetto ai quali non è possibile scendere in dettagli in questa sede, ma che possono assumere un rilievo importante in relazione a talune fattispecie concrete.

Al di fuori di tali strumenti, rimane comunque aperto, in via residuale, il ricorso al mezzo tradizionale della *rogatoria*.

Com'è noto, le rogatorie sono quelle richieste che uno Stato presenta a un altro per il compimento di determinati atti (comunicazioni, notificazioni, o – per quanto qui interessa – attività di acquisizione probatoria). Esse sono regolate, nel diritto interno, dagli artt. 723 e seguenti del codice di procedura penale. Tale disciplina, invero, è conforme alla fisionomia delle rogatorie sul piano internazionalistico, per la quale esse sono atti di dialogo fra Stati, e non fra autorità giudiziarie di Paesi diversi.

È una struttura che vede protagonisti gli esecutivi, in veste di rappresentanti, sul piano internazionale, dello Stato. Il modello conseguente è dunque quello per il quale la richiesta di rogatoria, sia in entrata, sia in uscita, deve transitare dal "filtro" dell'autorità politico-amministrativa (per l'Italia, il Ministero della Giustizia), avente poteri di diniego in parte anche discrezionali. E così, similmente, anche la controparte straniera utilizzerà un modello simile, proponendo come interlocutore diretto la struttura ministeriale.

Si tratta di un meccanismo che, interponendo un (doppio) controllo politico ai rapporti tra organi giurisdizionali, assicura agli Stati un considerevole grado di controllo nel proprio ambito sovrano, a spese tuttavia di quella certezza nella risposta, e – in caso di riscontro positivo da parte dell'autorità straniera – di agilità e rapidità nell'esecuzione, che il passaggio attraverso le strutture politico-amministrative di entrambi i Paesi non può che pregiudicare.

Come accennato, l'evoluzione degli strumenti di cooperazione giudiziaria internazionale in materia di *cybercrime*, mossa dalla necessità di strumenti operativi certi, agili e veloci, ha finora trovato svolgimento in due contesti multilaterali: il Consiglio d'Europa e l'Unione europea.

Quanto al primo, va anzitutto ricordata la Convenzione di Budapest (cd. *Cybercrime*) del 23.11.2001, recepita in Italia con l. n. 48/2008; nonché recentissimamente, il Secondo Protocollo addizionale alla Convenzione di Budapest, adottato il 17.11.2021, aperto alle firme il 12.5.2022, non ancora entrato in vigore.

Quanto invece all'ambito eurounitario, va ricordata già la Convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea (cd. "Bruxelles") del 29.5.2000, recepita tuttavia molto tardivamente in Italia, con d.lgs. n. 52/2017; nonché, più di recente, la direttiva n. 41/2014, trasposta con d.lgs. n. 108/2017, in materia di ordine europeo di indagine.

Si tratta di strumenti di cooperazione molto diversi tra loro, sotto più profili. Quanto alla materia, se i testi in ambito di "Grande Europa" sono dedicati specificamente al *cybercrime*, quelli di matrice UE hanno invece carattere assolutamente generale. È poi diversa la platea dei destinatari, molto più ampia per la Convenzione *Cybercrime* rispetto agli Stati membri dell'Unione vincolati dalla Direttiva. Infine, cambia il livello di intensità della cooperazione, più stretta in sede eurounitaria, anche se – come detto – operante fra un minor numero di Stati.

Lo strumento internazionale in materia fino ad oggi più importante, nonché quello storicamente più risalente, è senza dubbio la citata *Convenzione di Budapest*.

Benché sia stata trasposta nell'ordinamento interno soltanto nel 2008, nonostante fosse stata adottata nel 2001, il suo rilievo è stato enorme sul piano internazionale, soprattutto in ragione dell'elevato numero di Paesi aderenti – attualmente oltre sessanta – con una platea che si è negli anni allargata anche a Stati non appartenenti al Consiglio d'Europa ma dal rilievo strategico fondamentale. Ne fanno parte, per tutti, il Giappone, il Canada e – soprattutto

– gli USA, in cui hanno sede legale moltissime fra le maggiori piattaforme e *provider*. Allo stato, come tale, esso è dunque il testo maggiormente condiviso da parte della comunità internazionale, pur non potendo ancora ambire a quel carattere di quasi-universalità tipico delle convenzioni stipulate in seno alle Nazioni Unite.

Scendendo nel dettaglio, la Convenzione *Cybercrime* colloca le norme in materia di cooperazione giudiziaria (artt. 23-35) di seguito a quelle di armonizzazione delle fattispecie sul piano del diritto penale sostanziale (artt. 2-13) e degli strumenti di indagine a livello procedurale (artt. 14-22).

Il principio di fondo espresso dalla Convenzione in materia è quello del massimo favore per la cooperazione internazionale. Le Parti, in particolare, si impegnano a un generale dovere di collaborazione "*nella misura più ampia possibile nelle indagini o nei procedimenti riguardanti reati collegati a sistemi e dati informatici*" (art. 23), nonché di mutua assistenza per le medesime fattispecie (art. 25).

Simili clausole programmatiche, di *soft law*, trovano attuazione nella disciplina puntuale che regola i meccanismi di *mutual assistance* (art. 27). È previsto che ogni aderente designi "*un'autorità centrale responsabile dell'invio e delle risposte alle richieste di mutua assistenza, dell'esecuzione di tali richieste o della loro trasmissione alle autorità competenti per la loro esecuzione*", e che tali autorità centrali debbano comunicare direttamente tra loro. Tuttavia, "*in caso di urgenza, le richieste di mutua assistenza o le comunicazioni ad essa collegate possono essere trasmesse direttamente alle autorità giudiziarie della Parte richiedente dalle autorità della Parte richiesta*".

Per facilitare l'autorità inquirente di uno Stato nell'attivare tali strumenti di mutua assistenza, è previsto che ogni aderente alla Convenzione istituisca un punto di contatto, reperibile 24 ore su 24 e 7 giorni su 7 (art. 35). Quest'ultimo ha il compito di prestare immediato ausilio agli inquirenti stranieri, anche in relazione alla disciplina interna, nella presentazione di richieste di mutua assistenza ai sensi dell'art. 25, nonché di provvedere direttamente – ove il diritto interno lo consenta – a raccogliere prove o localizzare sospetti.

In sintesi, la Convenzione *Cybercrime*, pur consentendo dei momenti di contatto diretto tra autorità giudiziarie dei diversi Paesi, rimane ancora a ben vedere in parte legata al modello della rogatoria. Il meccanismo standard di mutua assistenza, infatti, transita ancora dal dialogo tra autorità centralizzate.

Certo, vi è anche da dire come le aperture a meccanismi più snelli di cooperazione, permesse dal carattere flessibile di molte previsioni del testo convenzionale, siano state tendenzialmente poco valorizzate, mediante scelte – in

sede di trasposizione – affatto progressive. Basti pensare, una per tutte, come l'"autorità centrale" scelta dall'Italia in sede di trasposizione della disciplina convenzionale, a mente dell'art. 13 d.lgs. n. 48/2008, sia ancora – come nel meccanismo classico della rogatoria – il Ministero della Giustizia.

Il diverso versante degli strumenti di matrice eurounitaria relativi alla cooperazione giudiziaria in materia penale, di rilievo anche rispetto al tema del *cybercrime*, ha a lungo scontato una marginalizzazione rispetto all'*acquis* comunitario più tradizionale. La Convenzione di Bruxelles del 2000, sopra ricordata, è intervenuta probabilmente in una fase in cui l'integrazione europea, sul punto, non era sufficientemente matura, e non ha avuto un seguito di particolare rilievo. In Italia, la Convenzione è rimasta inattuata per diciassette anni, e recepita soltanto pochi mesi prima che venisse recepita la più incisiva direttiva n. 41/2014, che nel frattempo era stata approvata, che ha introdotto l'*ordine di indagine europeo*.

Come noto, l'OIE (in inglese *European Investigation Order*, EIO) è, secondo la definizione dell'art. 1 della direttiva 41/2014, una decisione giudiziaria emessa o convalidata da un'autorità competente di uno Stato membro (lo "Stato di emissione") per compiere uno o più atti di indagine specifici in un altro Stato membro (lo "Stato di esecuzione") al fine di acquisire prove o di ottenere prove già in possesso delle autorità competenti dello Stato di esecuzione.

La procedura ha carattere «orizzontale» ed è ben più fluida. A mente dell'art. 7, l'OIE è trasmesso dall'autorità di emissione all'autorità di esecuzione con ogni mezzo che consenta di conservare una traccia scritta in condizioni che permettano allo Stato di esecuzione di stabilirne l'autenticità. La trasmissione è effettuata direttamente all'autorità di esecuzione, la quale è definita come "*un'autorità competente a riconoscere un OIE e ad assicurarne l'esecuzione conformemente alla presente direttiva e alle procedure applicabili in un caso interno analogo*" (art. 2 lett. d). Addirittura, la direttiva n. 41/2014 ha espressamente previsto l'adozione di una modulistica comune attraverso cui predisporre materialmente l'OIE, modulistica allegata anche al d.lgs. n. 108/2017. Va poi ricordato il ruolo di *Eurojust*, fra i cui compiti rientra anche quello di prestare assistenza nelle procedure di preparazione e invio degli OIE.

Le autorità giudiziarie, dunque, attraverso l'OIE dialogano direttamente tra loro, e non vi è normalmente alcun passaggio da una dimensione centralizzata, politica.

L'indubbia maggior agilità dello strumento e maggiore intensità della cooperazione che esso impone, che pure conducono a importantissimi frutti

in altri ambiti di reati, scontano tuttavia, quanto al settore del *cybercrime*, la circostanza per cui l'OIE consente di collaborare soltanto con gli Stati membri dell'Unione: o, più esattamente, tutti eccetto Danimarca e Irlanda, ai quali la menzionata direttiva non si applica. Si tratta di un'eccezione di non poco conto, in materia, se si considera che moltissime multinazionali di *internet* (per tutte, *Facebook*) hanno sede operativa per l'Europa proprio in Irlanda.

Non è dunque un caso come le energie riformatrici circa la cooperazione giudiziaria internazionale in materia di *cybercrime* si siano concentrate sul versante della Convenzione di Budapest, trattato – come detto – "di successo", essendo stato adottato sostanzialmente da tutti i maggiori soggetti del "blocco occidentale".

Il prodotto finale di tale sforzo è il *Secondo Protocollo addizionale alla Convenzione di Budapest*, il cui testo è stato adottato il 17.11.2021. Esso è stato aperto alla firma, sotto la presidenza italiana del Comitato dei Ministri del Consiglio d'Europa, il 12.5.2022. In tale sede, già ventidue Stati (fra cui anche gli USA) lo hanno sottoscritto, e in seguito dovrebbero pervenire le prime ratifiche. È previsto che il trattato entrerà in vigore sul piano internazionale al raggiungimento di cinque ratifiche. Sul piano interno, occorrerà poi ovviamente una normativa di recepimento.

Il percorso riformatore della Convenzione *cybercrime* è stato lungo e articolato. Nei vent'anni successivi alla stipula della Convenzione il contesto criminologico si è evoluto enormemente, al punto da imporre fin quasi da subito la necessità di aggiornarne il testo, in particolare sul tema della cooperazione giudiziaria.

La stessa Convenzione, consapevole di ciò, aveva previsto l'istituzione di una commissione permanente – la *Cybercrime Convention Committee* (T-CY) – che avrebbe dovuto svolgere il ruolo propulsivo, sul piano tecnico, rispetto ai necessari aggiornamenti. A seguito dei lavori di alcuni sottogruppi (*Transborder Group*, 2012; *Cloud Evidence Group*, CEG, 2015) si è pervenuti ad indicare le questioni del *cloud computing*, della territorialità e della giurisdizione quali principali nodi su cui lavorare per tentare di ovviare alle difficoltà degli inquirenti ad accedere fruttuosamente alle prove informatiche.

Le Alte Parti hanno deciso di incaricare la T-CY di preparare una bozza di Protocollo, limitandone l'oggetto alla questione della cooperazione giudiziaria, avvertita politicamente come prioritaria. Da ciò ha preso l'avvio il percorso articolato che ha condotto alla redazione del testo definitivo del Secondo Protocollo.

Per quanto questo non sia ancora in vigore, è interessante esaminare le novità che esso prevede rispetto al passato.

Anzitutto, il Protocollo prevede un meccanismo di collaborazione diretta con *provider* riferibili ad altri Paesi firmatari, per cui le autorità giudiziarie potranno chiedere l'identificazione di soggetti che abbiano registrato un dominio internet (art. 6) oppure informazioni in loro possesso circa un fruitore di loro servizi (art. 7).

È poi previsto un meccanismo di collaborazione diretta, «orizzontale», tra autorità inquirenti circa richieste di traffico dati (art. 8) oltre alla possibilità di chiedere direttamente, in caso di emergenza, assistenza nell'ottenimento da un *provider* riferibile a quel Paese informazioni in suo possesso (art. 9).

Infine, sono previste procedure di *mutual assistance* di emergenza, dove però il presupposto emergenziale è sostanzialmente autodichiarato dal richiedente, con obbligo delle Parti di garantire un'autorità con reperibilità costante al fine di evadere simili richieste urgenti (art. 10).

In sintesi, la disciplina risultante è di non poca complessità, cesellata con cura in sede di trattative tra le Parti. Complessivamente, non si giunge – ed evidentemente non si può politicamente giungere, allo stato, data la platea così ampia di Stati coinvolti – a un meccanismo semplice e generalizzato come quello dell'OIE.

Tuttavia, va rilevato come i meccanismi di collaborazione diretta – non solo tra autorità giudiziarie, ma addirittura direttamente con i *provider* stranieri – contemplati dal Secondo Protocollo, molto puntuali, specifici, riguardano proprio quel tipo di richieste la cui evasione tempestiva è sovente indispensabile per condurre in porto l'indagine, e dunque si può immaginare avranno significative ripercussioni nella prassi. Si può in effetti presumere che molti Stati (anche extraeuropei) sede dei principali *provider* di *internet* aderiranno allo strumento internazionale.

Sarà determinante – ai fini del "successo" del protocollo – verificare l'effettiva ratifica e implementazione dello strumento internazionale da parte di importanti *player* a livello globale, anzitutto gli USA. Allo stato, pare potersi affermare come la tempestiva implementazione del Protocollo sia un obiettivo fondamentale nella lotta al *cybercrime*, considerate le potenzialità dei nuovi strumenti di cooperazione offerti.

Invero, vi sono anche rilievi negativi che possono formularsi, che attengono, anzitutto, alla prevedibile lunghezza (viste le pregresse esperienze) dei tempi che occorreranno per l'entrata "a regime" dei nuovi strumenti – che forse non è del tutto inevitabile – la quale rischia di vanificare i progressi compiuti, permettendo alla fenomenologia criminosa di riaccumulare quel "vantaggio" strategico che il Protocollo mira invece a ridurre.

Poi, va detto come dal testo definitivo siano stati espunti interessanti

strumenti di cooperazione e indagine, invece presenti nei *draft* usciti dalle mani dei tecnici, con particolare riferimento ai temi delle operazioni sotto copertura in materia informatica e delle indagini tramite *transborder access*. Simili novità sarebbero state di grande utilità nelle indagini in materia di *cybercrime*, e l'occasione mancata del Secondo Protocollo determinerà, con tutta probabilità, la persistenza nel futuro di un interesse riformatore attorno alle tematiche sopracitate nel quadro della cooperazione internazionale.

Bibliografia e fonti

In letteratura, per tutti, possono ricordarsi:

– Cadoppi - Canestrari - Manna - Papa (diretto da), *Cybercrime*, Utet-Wki, Milano, 2019;

– Cajani - Costabile (a cura di), *Gli accertamenti informatici nelle investigazioni penali: una prospettiva europea*, Experta, Forlì, 2011;

– Marandola (a cura di), *Cooperazione giudiziaria europea in materia penale*, Giuffrè, Milano, 2018;

– Marchetti - Selvaggi (a cura di), *La nuova cooperazione giudiziaria penale. Dalle modifiche al codice di procedura penale all'ordine europeo di indagine*, Cedam-Wki, Milano, 2019;

– Mattarella, *La futura convenzione ONU sul cybercrime e il contrasto alle nuove forme di criminalità informatica*, in *Sistema penale*, 2/2022, pp. 41 ss.;

– Parodi - Sellaroli (a cura di), *Diritto penale dell'informatica. Reati della rete e sulla rete*, Giuffrè Francis Lefebvre, Milano, 2020.

Fondamentale, per l'approfondimento del tema, lo studio diretto delle fonti convenzionali, nonché dell'ampio materiale preparatorio e di analisi a cura di organi o commissioni delle istituzioni (T-CY, ecc.). Esso è reperibile direttamente sui siti istituzionali:

– *https://www.coe.int/en/web/cybercrime*, curatissimo sito del Consiglio d'Europa relativo agli strumenti convenzionali contro il *cybercrime*; cfr. in particolare gli *explanatory reports* relativi alla Convenzione di Budapest stessa e al Secondo Protocollo (*https://rm.coe.int/special-edition-budapest-convention-en-2022/1680a6992e*);

– *https://rm.coe.int/special-edition-second-protocol-en-2021/1680a69930*);

– *https://www.ejn-crimjust.europa.eu/ejn2021/Home/EN*, sito dello *European Judicial Network*, ricco di informazioni, nonché *https://www.eurojust.*

europa.eu, sito istituzionale di *Eurojust*;

– *https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home*, sui lavori della *ad hoc committee* istituita dall'ONU per la progettazione di una futura convenzione globale in tema di *cybercrime*.

Gli strumenti di cooperazione internazionale di polizia nella lotta al *cybercrime*

di Stilian Cortese*

La lotta ai fenomeni di cybercrime non può rimanere circoscritta al territorio nazionale, ma presuppone lo sviluppo di una sistematica e sinergica azione di contrasto anche al di fuori dello Stato italiano.

Di conseguenza, la collaborazione tra Autorità giudiziarie e Forze di Polizia di tutto il mondo è divenuta assolutamente necessaria per contrastare tali fenomeni, intercettarne le fonti di finanziamento e aggredirne i patrimoni illecitamente accumulati.

In un simile contesto, la conoscenza degli strumenti info-investigativi e giuridici esistenti in ambito domestico e globale assume una valenza decisiva, attesa l'esigenza di:

– incentivare sempre di più l'attività di scambio info-operativo, di supporto e coordinamento delle indagini, anche al di fuori dei confini statali, allo scopo di consentire l'acquisizione di elementi probatori e dare esecuzione a provvedimenti giudiziari/amministrativi all'estero;

– apprezzare vantaggi e svantaggi dei diversi strumenti che si sovrappongono e si intersecano, in modo da indirizzare sapientemente le scelte investigative.

Le due possibili tipologie di cooperazione internazionale sono:

– quella convenzionale/legale tra polizie, imperniata, da un lato, sul network dell'Organizzazione Internazionale di Polizia Criminale (INTERPOL), dall'altra, prevista da regolamenti comunitari e convenzioni ratificate dall'Italia, incentrata sulle piattaforme di cooperazione EUROPOL, S.I.Re.N.E. (Supplementary Information Request at the National Entries), A.R.O. (Asset Recovery Office) e Centri di Cooperazione di Polizia e Dogana (C.C.P.D.). Nel nostro Paese, tale tipologia di cooperazione viene sviluppata attraverso il Ministero dell'Interno - Direzione Centrale della Polizia Criminale - Servizio per la Cooperazione Internazionale di Polizia (S.C.I.P.);

– quella informale, basata sulla spontanea attività bilaterale di scambio informativo, in assenza di specifici strumenti di diritto internazionale.

In tale ambito – oltre ai numerosi accordi bilaterali stipulati dal Corpo della Guardia di Finanza con le omologhe agenzie di *law enforcement* e

(*) Tenente Colonnello della Guardia di Finanza.

ai rapporti di interscambio con i Legal Attaché delle Forze di Polizia estere presenti presso le Ambasciate a Roma – particolare rilevanza assume la rete degli Esperti della Guardia di Finanza, dislocata presso le principali Rappresentanze diplomatiche italiane all'estero.

Con riferimento al ruolo di INTERPOL, si evidenzia come l'Organizzazione in parola sia dedita alla cooperazione di polizia e al contrasto del crimine internazionale. Nata nel 1923 come Commissione internazionale di polizia criminale (International Criminal Police Commission), nel 1946 adottò come indirizzo telegrafico Interpol, contrazione delle parole inglesi international police (polizia internazionale), e dieci anni più tardi cambiò la denominazione ufficiale in The International Criminal Police Organization - INTERPOL, spesso abbreviata in ICPO-INTERPOL.

Attualmente si compone di 190 Paesi membri ed ha sede a Lione (Francia). L'Italia vi ha aderito definitivamente nel 1947.

In ogni Paese membro è presente un ufficio centrale di polizia internazionale, che collabora con le altre sezioni, con i corpi locali di polizia e con il Segretariato generale di Lione per la ricerca di chi ha commesso reati all'estero, o vi si è trasferito, e per la repressione della criminalità operante su scala internazionale. In particolare, l'INTERPOL è competente per le richieste di natura "puntuale".

Parallelamente, EUROPOL è l'agenzia dell'Unione europea incaricata dell'applicazione della legge, il cui obiettivo principale è quello di contribuire a realizzare un'Europa più sicura a beneficio di tutti i cittadini.

Con sede a L'Aia, nei Paesi Bassi, Europol fornisce assistenza ai 27 Stati membri dell'Unione europea nella loro lotta contro la grande criminalità internazionale e il terrorismo. L'agenzia collabora anche con molti Stati partner non membri dell'UE e con organizzazioni internazionali.

La posizione dell'agenzia, al centro dell'architettura della sicurezza europea, le consente di offrire una gamma unica di servizi e di fungere da:

- centro di sostegno per le operazioni di contrasto;
- centro informazioni sulle attività criminali;
- centro di competenze in tema di applicazione della legge.

L'analisi costituisce il cuore delle attività di Europol. L'agenzia impiega circa 100 analisti criminali che sono tra i migliori formati in Europa e utilizzano strumenti all'avanguardia per sostenere quotidianamente le indagini svolte dalle autorità incaricate dell'applicazione della legge negli Stati membri. Al fine di permettere ai nostri partner una maggiore comprensione dei crimini che si trovano ad affrontare, Europol produce delle valutazioni periodiche che offrono delle analisi esaustive e lungimiranti della criminalità

e del terrorismo nell'UE.

Con espresso riferimento al contrasto delle fenomenologie criminali legati al cyber, EUROPOL ha istituito l'European Cybercrime Centre (EC3) per rafforzare la risposta delle forze dell'ordine al cyber crimine e contribuire a proteggere i cittadini e le imprese europee. Infatti, la creazione di un centro europeo per la criminalità informatica era diventata una priorità nella strategia di sicurezza interna dell'UE e il posizionamento dell'European Cybercrime Centre all'interno di Europol ha significato una continuazione di alcune funzioni e un significativo ampliamento già in atto da diversi anni, in particolare dal punto di vista operativo e di supporto analitico alle indagini degli Stati membri.

Al fine di addentrarsi sempre più all'interno della specificità dei crimini informatici sono state create nuove funzioni specifiche per l'istituzione dell'European Cybercrime Centre. Oggi, quindi, l'EC3 è predisposto per concentrarsi principalmente su tre aree:

– reati informatici commessi da gruppi della criminalità organizzata, in particolare quelli che generano grandi profitti criminali come le frodi online;

– crimini informatici che causano gravi danni alle loro vittime, come lo sfruttamento sessuale dei minori online;

– crimini informatici (compresi gli attacchi informatici) che colpiscono infrastrutture critiche e sistemi informativi nell'Unione.

In merito a queste tre aree di monitoraggio, l'European Cybercrime Centre si pone come collettore di varie funzioni come:

– fungere da hub centrale per informazioni e intelligence criminali;

– sostenere le operazioni e le indagini degli Stati membri mediante analisi operative, coordinamento e competenze;

– fornire una varietà di prodotti di analisi strategica che consentano di prendere decisioni informate a livello tattico;

– stabilire una funzione di sensibilizzazione completa che colleghi le forze dell'ordine relative alla criminalità informatica;

– sostenere la formazione e il rafforzamento delle capacità, in particolare delle autorità competenti degli stati membri;

– fornire capacità di supporto tecnico forense digitale altamente specializzate alle indagini e alle operazioni di polizia giudiziaria;

– rappresentare la comunità delle forze dell'ordine dell'UE in aree di interesse comune (requisiti di R&S, governance di Internet).

Anche se Europol era attivo già da molti anni a supporto degli Stati membri nelle indagini nei vari ambiti di criminalità informatica, la continua-

zione dei lavori nell'ambito dell'European Cybercrime Centre ha subito uno sviluppo notevole. Considerando che tali indagini in passato avevano un focus prevalentemente nazionale con alcuni collegamenti internazionali, l'enfasi è stata progressivamente spostata verso il coordinamento delle operazioni internazionali di criminalità informatica, che hanno richiesto lo sviluppo di cooperazione attraverso l'EC3. In tutte le aree di competenza dell'European Cybercrime Centre la dimensione, la complessità e il numero di operazioni a cui far fronte è aumentato in modo significativo. Ciò ha portato ad intensificare gli sforzi e ad attuare più azioni investigative con conseguenti arresti e messe in stato di accusa per i responsabili.

Una particolare attenzione viene posta dall'European Cybercrime Centre nei confronti dei mercati criminali presenti nel dark web. Negli ultimi anni diverse indagini coordinate sono state in grado di abbattere alcuni dei più grandi mercati del dark web, minando le risorse sfruttate dai criminali.

In tale contesto, ad esempio, nell'ottobre del 2021, il Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della Guardia di Finanza di Roma ha concluso una sofisticata indagine tecnica nel mondo dei Black Market del Dark Web individuando gli amministratori del noto DeepSea, una piattaforma di vendita on-line di ogni genere di merce illegale, sotto il coordinamento della Procura della Repubblica di Brescia. Questo importante risultato, grazie anche all'apporto fornito dal II Reparto del Comando Generale della Guardia di Finanza per i rapporti di collaborazione internazionale tra le Forze di polizia, si inquadra nell'ambito dell'operazione "Dark Huntor" promossa da Europol per sensibilizzare l'opinione pubblica sui pericoli connessi alla navigazione nel Dark Web e all'acquisto di merce illegale sui Black Market, oltre che per sottolineare il costante impegno nel settore da parte delle Forze di polizia europee. L'indagine, avviata nel corso del mese di luglio 2020, ha consentito di identificare in provincia di Modena un soggetto attivo nel riciclaggio di criptovalute oltre che ideatore e creatore di un Black Market del Dark Web, denominato DeepSea, e di trarlo in arresto unitamente ad un altro soggetto. Nel corso dell'operazione sono stati sequestrati anche Bitcoin (BTC) e Monero (XMR), per un controvalore di circa 3,6 milioni di Euro, n. 3 autovetture di lusso per circa 370.000 Euro, n. 9 orologi di marca per circa 90.000 Euro, oltre a vari dispositivi informatici utilizzati per commettere i reati. I personal computer, notebook e smartphone sequestrati nel corso dell'operazione sono stati esaminati secondo le migliori tecniche di analisi forense per ricostruire sia le attività illegali compiute attraverso il Black Market che i movimenti di valuta virtuale connessi agli scambi illegali realizzati con la piattaforma. I Bitcoin e i Monero sono infatti le monete virtuali molto diffuse nel mondo

dell'illegalità connessa ai traffici illeciti nel Dark Web e alle attività di riciclaggio di "denaro sporco", attività in grado di rendere guadagni di migliaia di euro mensili. Come noto, i Black Market del Dark Web sono risorse informatiche accessibili solo utilizzando browser che consentono di navigare in rete in completo anonimato (browser TOR con dominio .onion). Le risorse del Dark Web non vengono indicizzate dai comuni motori di ricerca e non sono registrate presso i pubblici registri dei domini in quanto finalizzate a garantire l'anonimato degli utenti che vi navigano. Per ottenere questo risultato la connessione viene fatta "rimbalzare" tra più server, ubicati in Stati diversi, chiamati nodi, in modo da rendere pressoché impossibile rintracciare la sua reale origine. Inoltre, i dati scambiati vengono criptati tra un nodo e l'altro. L'accesso non è libero ma ristretto agli utenti accreditati. I Black Market si presentano come un vero e proprio mercato on-line in cui i numerosi venditori (vendor) pubblicizzano e propongono in vendita merci e servizi illegali. La creazione di un account su tali portali è impostata su username e password, in totale anonimato. Considerando la peculiarità della merce posta in vendita, l'utilizzo dei Black Market rende estremamente pericolose le risorse in questione, poiché si rivolgono ad una vasta platea di acquirenti e venditori, essendo accessibili da soggetti di tutto il mondo e di qualsiasi fascia di età. Peraltro, l'acquisto di merce illegale sui Black Market, oltre a configurare precise violazioni di legge, anche molto gravi, espone gli acquirenti a ulteriori rischi connessi alla condivisione di dati personali con soggetti privi di scrupoli che possono riutilizzarli in altri contesti parimenti illegali, alla possibilità di "infettare" i propri apparati informatici con virus e malware dannosi, oltre alla eventualità che i prodotti acquistati siano diversi da quelli attesi o che la merce ordinata non venga recapitata affatto. Gli investigatori sono riusciti ad individuare i soggetti coinvolti nella gestione del Black Market del Dark Web denominato DeepSea, che funzionava con le stesse modalità di un normale sito di e-commerce, con la differenza che gestiva e promuoveva la vendita di prodotti di natura illecita, sfruttando l'anonimato del protocollo Tor, caratteristico del Dark Web. Sono stati riscontrati più di 1.000 vendor accreditati e più di 110.000 clienti/acquirenti. Nel corso di circa 6 mesi sono stati registrati circa 70.000 ordini di acquisto, di cui oltre 45.000 riferiti alle sole sostanze stupefacenti. I prodotti in vendita erano organizzati nelle seguenti categorie:

– n. 643 annunci di servizi relativi ai cosiddetti "Bank Drops", servizi per i quali un intermediario si offre di effettuare una transazione su un conto corrente indicato dal cliente, dietro pagamento di una commissione pari ad una certa percentuale della transazione effettuata. Tale servizio viene generalmente richiesto quando si vuole celare la provenienza di una certa disponibi-

lità finanziaria (anche in bitcoin) che verrà inviata all'intermediario, il quale provvederà a recapitare la somma al destinatario finale tramite un tradizionale bonifico bancario da un conto corrente "pulito" a sua disposizione;

– n. 57 annunci relativi a documenti di identità, nazionali ed esteri, riportanti i segni distintivi dei rispettivi Paesi. Vi erano diverse tipologie di documenti posti in vendita, materiali o digitali. Nel caso dei documenti di identità digitali, vi era la possibilità da parte dei clienti di acquistare i cosiddetti template, ovvero veri e propri file editabili sui quali inserire dati anagrafici e fotografie a piacimento degli utilizzatori finali, per poi stampare un numero illimitato di documenti falsi;

– 8.349 annunci di vendita relativi a farmaci e sostanze stupefacenti suddivisi in: Cannabis &Hashish, psicofarmaci, farmaci, ecstasy, oppioidi, oltre alla cocaina e all'eroina;

– 444 annunci riguardanti la vendita di oro, argento ed altri prodotti di gioielleria, verosimilmente di provenienza illecita o contraffatti;

– 340 annunci di malware, tra cui virus informatici, Botnet, Exploits, VPN utili a celare il proprio indirizzo IP, strumenti per incrementare le misure di sicurezza in termini di anonimato online, al fine, generalmente, di camuffare la propria identità virtuale per il compimento di scopi illeciti o bypassare blocchi governativi;

– 3.255 annunci di carte di credito clonate.

Intelligenza artificiale, influenza sul mercato politico e reati contro la personalità dello Stato. Profili generali

di Claudio Orazio Onorati*

1. Introduzione

Il tema dell'utilizzo dell'Intelligenza Artificiale (I.A.) nei delitti contro la Personalità dello Stato e dell'influenza sul mercato politico involge una molteplicità di aspetti che giungono a toccare categorie di diritto costituzionale, poiché tali fenomeni sono in grado di incidere ormai – per complessità delle forme di manifestazione e per "scala" degli attacchi – sulla fruizione e sul godimento delle più importanti libertà civili (artt. 2-3, 13-21, 48 Cost.) quali: il diritto di manifestazione libera del pensiero; il diritto di manifestazione delle proprie convinzioni politiche; l'esercizio libero del diritto di voto e delle libertà civili, che possono essere minacciate nel loro pieno e libero svolgimento da nuovi fenomeni di devianza criminale che si compiono attraverso le reti e tramite strumenti che utilizzano I.A.

Già da alcuni anni, inoltre, sullo scenario globale della Cyberwarfare, sono emerse forme "subdole" di attacco e di influenza indebita tra Stati che attengono direttamente o indirettamente al tema dell'esercizio della Sovranità.

È soprattutto sotto questo profilo che si pongono i temi (penalistici soprattutto) dell'inquadramento e del trattamento repressivo di alcuni fenomeni di utilizzo "ideologizzato" e massivo dell'I.A. sia al fine di considerare il possibile inserimento di alcuni utilizzi "nocivi" dell'I.A. nell'ambito delle condotte e dei fenomeni di terrorismo ed eversione, sia al fine di valutare la tenuta delle attuali norme incriminatrici in materia di reati contro la personalità dello Stato e di contrasto al terrorismo, e dunque – più in generale – di apprezzare l'effettività e l'adeguatezza dell'intero sistema di regole penalistiche di fronte all'avanzata di inedite forme di devianza commesse con tecnologie all'avanguardia.

2. Scenari di Impiego Nocivo dell'I.A. (M.U.A.I.)

Vari sono gli scenari di possibile impiego nocivo degli strumenti di Intelligenza Artificiale (MUAI - Malicious Use of Artificial Intelligence) sia

(*) Sostituto Procuratore della Procura della Repubblica presso il Tribunale di Napoli.

mediante "attacchi diretti" – cioè attacchi informatici che utilizzino su larga scala la potenza di elaborazione e "reazione" dell'I.A. per realizzare danni ed eventi devastanti – sia mediante attacchi "indiretti" che possono sfruttare le potenzialità ma anche le stesse vulnerabilità dell'I.A. al fine di destabilizzare, influenzare, orientare in modo più o meno subdolo i sistemi politici e l'opinione pubblica, attraverso avanzate tecniche di profilazione e "disseminazione" in rete.

Sotto il primo aspetto (attacchi diretti) va considerato che l'enorme avanzamento tecnologico avuto negli ultimi anni in termini di attuazione degli algoritmi di AI negli ambiti pratici, e l'abbassamento delle barriere d'ingresso in termini di competenze tecniche richieste per il loro utilizzo, hanno reso appetibili l'I.A. anche per le organizzazioni terroristiche che puntano a usarle come vere e proprie risorse.

Sotto il secondo aspetto vengono invece in rilievo più specificamente i fenomeni della disinformazione tramite internet (fake news) e quello della 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'.

Di recente, diversi studi e documenti UE – ripresi anche dal rapporto UNICRI di maggio 2021[1] – hanno iniziato ad ipotizzare tra i possibili scenari di utilizzo distorto dell'AI sia quello di un utilizzo concreto di nuovi algoritmi nocivi per condurre e portare a termine (massimizzando) un attacco sui sistemi e infrastrutture critiche, sia quello di interventi per distorcere il funzionamento degli algoritmi esistenti e leciti allo scopo di "deviarne" le azioni e le risposte in modo coerente con finalità di orientamento, destabilizzazione o terroristiche.

Anche secondo tali fonti, l'impiego nocivo dell'I.A. (MUAI: "Malicious Use of Artificial Intelligence"[2]), specie per finalità terroristiche, può concretizzarsi in numerosi modi:

– sabotaggio dei sistemi integrati e onnicomprensivi di IA (es. infrastrutture, sistemi di trasporto robotici ad autoapprendimento con gestione centralizzata basata sulla IA), preziosi obiettivi per atti di destabilizzazione;

1) *Http://www.unicri.it/News/Algorithms-Terrorism-Malicious-Use-Artificial-Intelligence-Terrorist-Purposes.*
2) Cfr. M. Brundage et al., 2008, per l'espressione "*Malicious Use of Artificial Intelligence*" - MUAI, 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).

– ri-orientamento ad opera del terrorismo dei sistemi commerciali di IA 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.

3. Disinformazione: il fenomeno espansivo delle *deep fakes* e dei *social bots*

Con il termine "Disinformazione" si intende comunemente il fenomeno della divulgazione o diffusione di notizie od opinioni false o fuorvianti attraverso la somministrazione di dati o documenti apparentemente credibili.

L'origine dell'espressione verosimilmente ricondotta al termine russo "dezinformatzija" (дезинформация) che si riferisce ad un'arma tattica usata nella guerra sovietica sin dal 1923. Le misure attivate dall'intelligence sovietica si basavano sulla falsificazione come operazione segreta e sulla sovversione e manipolazione dei media.

Come noto, la disinformazione può prevedere la distribuzione di documenti falsi, manoscritti e fotografie, o la diffusione di voci maliziose e dossier creati appositamente. Simili espedienti vengono utilizzati anche nella competizione commerciale per indebolire la posizione di un concorrente, e perfino a livello governativo per tenere segrete verità altrimenti compromettenti, difficili da gestire, o con un forte impatto sull'opinione pubblica. Tecniche di disinformazione vengono usate comunemente anche nell'ambito del commercio e della vendita (marketing) di prodotti da parte di aziende e relativi venditori, anche nella forma di pubblicità ingannevole.

Di grande interesse è poi il filone dottrinario che tende a ricondurre alla macro-categoria della disinformazione anche il False Balance (falso equilibrio) anche detto bothsidesism, noto come un *bias* utilizzato dai media in cui i giornalisti nell'intento (o con il pretesto) di dare voce al pluralismo e di presentare una visione "più equilibrata" tra punti di vista opposti per ciascuna delle parti, in realtà presentano prove e argomentazioni sproporzionate rispetto alle prove effettive, oppure possono omettere informazioni che dimostrerebbero che le affermazioni di una parte sono prive di fondamento. Il falso equilibrio di solito deriva da un tentativo di evitare bias, ma dà a posizioni non supportate o dubbie un'illusione di rispettabilità e può creare la percezio-

ne nel pubblico che alcune questioni siano scientificamente controverse, anche se in realtà non lo sono, creando quindi dubbi che possono essere sfruttati da gruppi di interesse[3].

Con l'avvento delle nuove tecnologie, la categoria della disinformazione ha ricompreso anche le Fake news (letteralmente false notizie, notizie fasulle, o ancora pseudonotizie) con cui si indicano gli articoli o le pubblicazioni presenti e veicolate attraverso le reti e i social media redatti con informazioni inventate, ingannevoli o distorte, e rese pubbliche con il deliberato intento di disinformare o di creare scandalo attraverso i mezzi di informazione, oppure con lo scopo di attirare *click* su Internet.

4. L'Intelligenza Artificiale per la creazione e viralizzazione di "Deep Fakes"

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[4]. 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 IA 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[5]. 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[6].

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

3) Per esempio i temi della negazione del cambiamento climatico causato dall'uomo contro il cambiamento climatico naturale, gli effetti sulla salute del tabacco, la presunta relazione tra vaccini e autismo, le presunte cure contro la Covid-19 e l'evoluzione contro il design intelligente.

4) Definizione rinvenibile su *https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9512278* (accesso 11 novembre 2021).

5) 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 (accesso 11 novembre 2021).

6) *Ibidem*.

pochi secondi e senza confini.

Per identificare i deep fakes è spesso necessario l'utilizzo di speculari algoritmi di AI, che in via automatica sono in grado di intercettare i falsi.

Anche in questo caso, lo strumento tecnologico non è nato per scopi malevoli poiché vari sono gli ambiti di applicazione lecita dei deep fake che riguardano il mondo del cinema e dell'animazione , l'arte e l'intrattenimento in generale (es. avatar virtuali che agiscono parlando numerose lingue, ecc.). Ciò che preoccupa, invece, è la strumentalizzazione "malevola" del mezzo tecnologico, ma soprattutto la seriale disseminazione in rete del falso realizzato mediante deep fake, che grazie alle potenzialità dell'I.A. può avvenire in quantità e qualità tali da rendere sostanzialmente indistinguibile i fatti reali dall'artificiosa menzogna.

Inoltre, le tecniche di profilazione e di social engineering condotte su larga scala, facilitate dall'I.A. possono consentire oggi di individuare preventivamente categorie di soggetti "sensibili" o "fragili", ben predisposte a recepire il messaggio veicolato dall'attaccante e a fungere a sua volta da "cassa di risonanza" della macchina del falso.

In senso più ampio, il concetto arriva ad includere vere e proprie campagne di disinformazione, generate e amplificate nel web attraverso l'utilizzo simultaneo di numerosi canali informatici e telematici, che possono arrivare anche ad influenzare i meccanismi dei motori di ricerca e accreditano come vere informazioni o notizie false e costruite ad arte

L'impiego dei deep fake può essere associato a una varietà di manifestazioni illecite[7], corrispondenti anche nel nostro ordinamento a diverse fattispecie penali.

Si segnalano nei documenti citati in dottrina numerosi scenari di possibile utilizzo malevolo o illecito delle deep fake come:

– 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 mediante materiali pornografici o diffamatori rilasciati per colpire l'immagine e l'azione su singoli attori politici o contro di essi;

– estorsione (es. minaccia di rilasciare un video falso che danneggerebbe la reputazione o la credibilità di una persona fisica o giuridica);

7) 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 IA 'Malicious uses and abuses of AI', p. 52.

– distorsione e manipolazione dei mercati[8], ad esempio sia attraverso interventi diretti di algoritmi di IA (HFT - High Frequency Trading), sia attraverso diffusione di video e informazioni false in grado di condizionare l'andamento delle borse ovvero la diffusione di video falso in cui il CEO di una società quotata commette un reato o si lascia andare a commenti razzisti/misogini;

– incitamento agli atti di violenza contro minoranze, 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.

In questa direzione l'utilizzo di strumenti di I.A. da parte di movimenti estremisti può «rompere» lo schema tradizionale del rapporto intersoggettivo per attività di fidelizzazione e «attivazione» di cellule alla lotta armata e mette a disposizione strumenti di cui i gruppi terroristi si servono per smuovere l'emotività individuale o collettiva – in una escalation psicologica – e per creare un clima di incertezza, imprevedibilità e panico; nonché per viralizzare fake news o per crearne di nuove in modo sempre meno riconoscibili, in modo subdolo e con attività di profilazione dei big data, a livello globale.

In tal senso è stato notato che l'utilizzo di strumenti di I.A. può favorire e rendere meno riconoscibile la cyber-propaganda terroristica attraverso le attività di profilazione-georeferenziazione che permettono ai terroristi di individuare specifiche categorie di utenti particolarmente vulnerabili e suggestionabili alla manipolazione della propaganda, specialmente in caso di utilizzo di tecniche basate sulla "frequenza efficace" (cioè il numero medio di volte in cui i soggetti appartenenti al target group devono essere esposti a un messaggio o contattati nel corso di una campagna di fidelizzazione affinché diano una specifica risposta (es. per indurre un soggetto a unirsi alla lotta).

Le maggiori possibilità che gruppi privati e Stati accedano a tecnologie che utilizzano intelligenza artificiale per effettuare propaganda e interferenza nel mercato politico di altri Stati, per influenzarne la linea politica piuttosto che per sostenere o sovvertire le forme di Governo, in modo latente senza i problemi di "riconoscibilità" territoriale propri delle tecnologie tradizionali, rappresentano nuove minacce per beni costituzionalmente garantiti e per le libertà fondamentali dell'individuo, e pongono in discussione – anche sotto il profilo repressivo – la stessa sovranità dello Stato e le sue manifestazioni.

8) Sul tema cfr. nello specifico J. Bateman, *Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios*, luglio 2020.

Il problema, tutt'altro che teorico, si è già posto in una serie di casi in cui è tuttora discusso se alcune crisi politiche piuttosto che forme accese e violente di dissenso, siano state determinate e innescate dalla disseminazione di materiali costituenti deep fake.

Con tutte le riserve del caso dovute all'impossibilità di effettuare un riscontro di fact-checking sui materiali, tra i casi noti e dibattuti si possono citare i seguenti:

– accelerazione della crisi politica in Gabon nel 2018, quando fu postato in rete dal Governo locale un video del Presidente Bongo che fu oggetto di una intensa speculazione politica sul reale stato di salute del premier ed innescò il sospetto che il Governo locale stesse coprendo la cattiva salute o la morte di Bongo attraverso l'uso di deep fake, con conseguenti disordini, ed un tentativo di colpo di Stato, in cui fu richiamato proprio la pubblicazione del video;

– scandalo sessuale in Malesia nel giugno 2019, relativo ad un sex tape – tacciato di essere anche in questo caso una costruzione fittizia mediante deep fake e software di face morphing – che coinvolgeva presumibilmente il Ministro malese degli affari economici Azmin Ali e l'assistente maschile di un Ministro rivale, che provocò disordini e l'arresto del politico;

– manipolazione audio della voce di Nancy Pelosi con uno 'shallow fake': a marzo 2019 fu pubblicato in rete un video, poi risultato manipolato, con l'effetto di rallentare il discorso della Pelosi e sostenendo l'idea che la donna stesse biascicando le sue parole e che non fosse in sé. Il tutto allo scopo di rilanciarlo in rete e danneggiarne l'immagine politica[9]. Analogamente, Un video shallow fake è stato citato come prova della manipolazione di movimenti del corpo del giornalista effettuata al subdolo scopo per sostenere la legittimità della scelta politica di revocare l'accreditamento presso Casa Bianca del giornalista CNN Jim Acosta, scomodo per la Presidenza;

– 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 Welle (2020). Stando al rapporto, che cita fonti del Servizio Europeo per l'azione esterna dell'UE, la Russia avrebbe supportato il suo obiettivo finale di sovvertire le società

9) S. Mervosh, *Distorted Videos of Nancy Pelosi Spread on Facebook and Twitter, Helped by Trump*, in *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*, in *The Independent*, 24 maggio 2019.

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 includerebbe informazioni contraddittorie e notizie false come l'idea che il virus sia un'arma biologica statunitense (Avast 2020). A sua volta la Cina avrebbe rilanciato 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.

Rapporto COPASIR 2020 sull'infodemia durante la crisi del Covid-19 in Italia - IL CASO SPUTNIK E RUSSIA TODAY sugli interventi di Russia e Cina in Italia

Stando al rapporto i due Paesi, rientrerebbero fra quelli che hanno scelto di "cavalcare l'onda della disinformazione", cercando "in qualche modo di sfruttare l'emergenza per i propri interessi". Come nel caso dell'agenzia di stampa governativa russa Sputnik, che avrebbe diffuso contenuti "discutibili" attraverso i suoi canali internazionali, al fine di polarizzare le opinioni politiche e innescare insicurezza e disordine sociale. Tra i temi citati dal rapporto emergono: le "problematiche di ordine pubblico avvenute nei supermercati" ma anche "riferimenti espliciti ai fenomeni migratori"; la diffusione del coronavirus, raccontata come forma di aggressione straniera, originata in laboratori segreti; le teorie del complotto al fine di sfruttare il virus per scopi propri con l'obiettivo che in questo caso, è quello di creare sfiducia nei governi occidentali, nei loro sistemi sanitari e nel settore scientifico.

Stando al rapporto la Russia «come altri Stati, fa uso dell'informazione come "arma" per influenzare gli atteggiamenti, le credenze e le opinioni di leader e popolazione avversari, oltre che dei propri" ed aggiunge che tale influenza avverrebbe attraverso l'obiettivo di controllare i mass media, la politica, gli apparati militari, l'intelligence ed il settore energetico, all'interno di un contesto di guerra ibrida».

I casi di disinformazione che nel 2021 e 2022 sono stati individuati e segnalati anche dall'EDMO (European Digital Media Observatory e dall'IDMO (Italian Digital Media Observatory), da cui si può evincere come il tema della manipolazione dell'informazione a fini di propaganda o ricerca di consenso sia sostanzialmente "esploso" nel contesto politico Europeo con l'utilizzo di campagne "virali" di disinformazione realizzate col supporto di deep fake per diffondere materiali multimediali creati e manipolati con I.A. attraverso le principali piattaforme social allo scopo di contrastare la genuinità dell'informazione proveniente da canali e fonti "ufficiali", come quelli diffusi a seguito dell'inizio del conflitto Russo-Ucraino volti a sostenere le tesi della propaganda e disinfor-

mazione provenienti da fonti russe: es. videomessaggio del Pres. Zelensky che nei primi giorni di guerra annunciava la sua fuga e la resa delle sue truppe, in realtà proveniente da fonti russe; es. i video volti a sostenere le tesi che i morti e i feriti mostrati nelle città ucraine fossero in realtà costruiti con utilizzo di attori e con foto decontestualizzate (anche esse propaganda russa, come ad esempio il video sulla donna partoriente ferita, addirittura deportata e curata dai russi; il video manipolato dei cadaveri di BUcha che si muovevano dopo il passaggio del cameraman oppure quelli volti a sostenere in base a finti rilevamenti satellitari che fossero già in strada all'arrivo dei militari russi per accreditare la tesi del "fuoco amico" o della strage Ucraina; i video del Pres. Zelensky con cocaina sul suo tavolo (frutto di mix di video).

5. Il collegamento tra campagne no-vax, guerra e neonazismo da parte Ucraina

Analoghe questioni di interferenza sul mercato politico si pongono in relazione alla diffusione massiva, attraverso piattaforme social, di video ed altri materiali di presunta contro-informazione (in realtà disinformazione) su temi sensibili per l'opinione pubblica e "caldi" per l'agenda politica dei principali Governi Occidentali come ad esempio sembra essere avvenuto:

– per la pandemia di Covid-19, con la viralizzazione video manipolati e finti documenti volti a sostenere inefficacia dei vaccini contro il Covid, ovvero volti a propalare teorie del complotto al fine di accreditare l'idea dell'inefficacia o addirittura della dannosità dei vaccini e l'occultamento dei dati da parte dei Governi, asserviti al presunto volere dei colossi del "BIG PHARMA";

– per i temi ambientalisti come quello della riconversione energetica e dei cambiamenti climatici: in questo senso va citato il video pubblicato su piattaforma Tik Tok con il testo di un articolo intitolato "Evitare un blocco climatico", da un account che afferma che i Governi si adopereranno per limitare attività, spostamenti e consumi dei cittadini a vantaggio delle grandi imprese. Le condivisioni del video, anche al di fuori delle principali chat, lo portano a quasi 70.000 visualizzazioni. Nello stesso senso possono essere citati i video e le campagne dirette contro i leader del movimento ecologista, come l'adolescente Greta Thunberg, accusate, falsamente, di essere a libro paga di multinazionali e di classi privilegiate che si avvantaggiano delle precauzioni prese a tutela dell'ambiente.

6. La risposta penalistica: problemi, limiti e prospettive

L'avvento degli strumenti di AI 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.

Ma il vero interrogativo resta quello relativo alla possibilità di incriminare le condotte di viralizzazione di deep fakes e di interferenza sul mercato politico/finanziario con le norme esistenti in materia di terrorismo e in materia di reati contro la personalità dello Stato, dove la "tipicità del fatto" e della fattispecie sembrano attagliarsi ben poco a fenomeni non connotati da "eventi" ben individuati e identificabili empiricamente, bensì da eventi e condotte "diffuse", rilanciate da più attori che operano nello spazio virtuale in modo anche cronologicamente "remoto" rispetto agli effetti "a cascata" che hanno innescato direttamente.

6.1. Norme incriminatrici che possono essere applicate in caso di interferenze sul mercato politico e campagne di disinformazione attraverso *deep fake*

Come accennato, la risposta penale, con l'utilizzo delle sanzioni ordinarie già previste dall'ordinamento penale, è uno strumento delicato che deve

trovare applicazione – in ossequio al principio di *extrema ratio* – soltanto in caso di lesione di diritti fondamentali e di configurabilità del dolo intenzionale in capo al propagatore del falso.

Non essendo prevista alcuna fattispecie specifica non è però agevole individuare la fattispecie da applicare al fenomeno oggetto di analisi. Sul punto, anche la dottrina penalistica è divisa.

Tralasciando ipotesi minoritarie (es. quelle che si riferiscono all'art. 595 c.p. o all'art. 368 c.p.) e che appaiono deboli come quelle che puntano sulle fattispecie di vilipendio delle istituzioni della Repubblica (art. 290 c.p.) istigazione a delinquere (art. 414 c.p.), abuso della credulità popolare (art. 661 c.p.), più calzante appare la tesi che richiama la fattispecie di pubblicazione di notizie false, esagerate o tendenziose atte a turbare l'ordine pubblico (art. 656 c.p.), la cui difficoltà applicativa appare però palese.

Proprio con riferimento all'art. 656 c.p., che sembrerebbe idonea a colpire il fenomeno le fake news, in quanto reato di pericolo, per cui non occorre neppure che dalla condotta sia scaturito o meno un effettivo turbamento dell'ordine pubblico (cfr. Cass. Sez. 1 n. 9475, 22 ottobre 1997) va detto però che tale fattispecie è stata ridimensionata dalla Corte costituzionale che ha escluso il reato in caso di notizie «tendenziose» (cioè che fa riferimento a fatti veri, ma li rappresenta con modalità che offrono un'alterata rappresentazione del reale) così come ha precisato che non vi rientra la «divulgazione di interpretazioni, valutazioni, commenti, ideologicamente qualificati e perfino tendenziosi, riferiti a fatti veri».

Sul tema più specifico delle interferenze nella formazione del consenso e della volontà elettorale, oltre che dei procedimenti e meccanismi che regolano la manifestazione del consenso e della volontà popolare in occasione di competizioni elettorali e di esercizio del voto, viene poi in rilievo il delitto di cui all'art. 294 c.p. che incrimina "l'attentato contro i diritti politici del cittadino e che consiste nella violenza, minaccia o inganno che si traduce nell'impedimento all'esercizio di un diritto politico o nella determinazione del cittadino stesso ad esercitarlo in maniera difforme dalla sua volontà: diritti politici, nell'attuale assetto costituzionale, sono quelli che permettono al cittadino di partecipare all'organizzazione ed al funzionamento dello Stato e degli altri enti di rilevanza costituzionale, come le regioni, le province e i comuni, ai quali è attribuita la funzione di indirizzo politico in relazione ad un determinato aggregato di persone stanziate su una parte del territorio" (così Corte di Cassazione, sez. I, 14/10/1993). Tuttavia anche in questo caso l'elemento essenziale per la configurazione materiale del reato di cui all'art. 294 c.p. è costituito dall'impedimento di un diritto politico che deve essere

compiuto con un mezzo fraudolento che produca gli stessi effetti della violenza o della minaccia, cui è equiparato, in ordine all'"idoneità", il requisito di una pressione di tale intensità da indurre la p.o. a determinarsi nell'esercizio di un diritto politico in modo contrario alla sua reale volontà (Così Corte di Cassazione, sez. I, 26/06/1989).

6.2. Il difficile bilanciamento degli interessi costituzionali (art. 3-48 co. 2 Cost. e 21-27 Cost.) in caso di disinformazione e interventi sul mercato politico

La garanzia del genuino svolgimento delle competizioni elettorali, scevro da qualunque forma di indebita pressione e/o condizionamento, assurge dunque ad interesse primario in vista del corretto dispiegarsi delle regole democratiche di Governo, atteso che la partecipazione alla vita istituzionale dello Stato costituisce, al contempo, un diritto ed un dovere (morale) del cittadino, promuove il genuino perseguimento dell'interesse generale, rafforza e sviluppa il senso di appartenenza e condivisione dei valori in cui si sintetizza e realizza la sovranità popolare, garantisce, in definitiva, la libertà e l'uguaglianza di tutti[10].

Si comprende dunque quanto sia difficile bilanciamento da realizzare tra esigenze di tutela dell'ordine e della sicurezza pubblica e riconoscimento dei diritti di elettorato attivo e passivo, attributi indefettibili di una moderna democrazia, laddove sia possibile assistere a tentativi di alterazione e/o condizionamento del processo di formazione della volontà politica del corpo elettorale.

La predisposizione di norme incriminatici tese a prevenire, se possibile, o, comunque, reprimere i fenomeni di indebita influenza sul libero esercizio del diritto di voto – espressione, spesso, di illecite cointeressenze, ovvero di tentativi di assoggettare alla volontà delle organizzazioni criminali l'amministrazione della "cosa pubblica" – costituisce un indispensabile strumento di difesa delle libere istituzioni a fronte della pervicace ingerenza delle consorterie criminali verso fenomeni che possono compromettere il principio democratico previsto dall'articolo 48 della Costituzione.

Per converso, non si può non considerare che l'estensione dell'area delle incriminazioni vada in misura corrispondente ad incidere anche sull'area della libertà di critica e propaganda elettorale, sulle forme di manifestazione del dissenso, anche politico, della satira, che oggi si manifestano anche attra-

10) Cfr. L. Buscema, *Reati elettorali e principio di democraticità dell'ordinamento: profili assiologici e ricostruttivi*; in *Diritto Penale Contemporaneo*, 28.10.2013.

verso le nuove tecnologie. Esse sono indubbiamente tutelate dagli artt. 3-13 e 21 Cost.

Tale tema è caro anche alla Corte costituzionale che ne ha fatto ampia applicazione nelle pronunce "evolutive" in materia di libertà di manifestazione del pensiero, passando da una visione prevalentemente individualistica della libertà di manifestazione del pensiero (sent. n. 9 del 1965), definita anche «pietra angolare e fondamento dell'ordine democratico» (sent. n. 84 del 1969) con i suoi riferimenti alla libertà di espressione utilizzata per fini informativi, ha aperto ad una lettura funzionalista del diritto di manifestare il proprio pensiero, estendendo la tutela prevista dall'art. 21 Cost. anche al diritto "passivo" ad essere informati (a tutela del "pluralismo interno", tra le forze politiche, e del "pluralismo esterno", tra le diverse forme informative, C. Cost. sent. 153 del 1987, sent. n. 112 del 1993, sent. 155 del 2002).

Ma ciò ha modificato anche la nozione del diritto all'informazione garantito dall'art. 21 anche come diritto alla "corretta informazione" caratterizzato: a) dal pluralismo delle fonti cui attingere conoscenze e notizie – che comporta, fra l'altro, il vincolo al legislatore di impedire la formazione di posizioni dominanti e di favorire l'accesso (anche nel sistema radiotelevisivo del massimo numero possibile di voci diverse – in modo tale che il cittadino possa essere messo in condizione di compiere le sue valutazioni avendo presenti punti di vista differenti e orientamenti culturali contrastanti; b) dall'obiettività e dall'imparzialità dei dati forniti; c) dalla completezza, dalla correttezza e dalla continuità dell'attività di informazione erogata; d) dal rispetto della dignità umana, dell'ordine pubblico, del buon costume e del libero sviluppo psichico e morale dei minori» (C. Cost. sent. n. 112 del 1993)[11].

La garanzia della libertà di manifestazione del pensiero ex art. 21 Cost. non per questo giustifica la riconduzione de plano di ogni notizia falsa nell'alveo delle fake news.

Un punto cruciale è quello di individuare una sorta di definizione minima di fake news (e deep fake), che permetta di evitare ingiuste censure nel campo delle opinioni e della libera manifestazione del pensiero e che andrebbe limitata all'ipotesi di "notizie false" che sono intenzionalmente e verificabilmente false e che potrebbero fuorviare i lettori attraverso una consapevole diffusione finalizzata a fuorviarne la comprensione e interpretazione dei fatti.

La materia allo stato non è oggetto di una specifica disciplina penalistica, né sono ancora sul tappeto tutte le argomentazioni risolutive dell'ampio dibattito dottrinario che suggerisce anche il superamento di una tale prospetti-

11) F. Sammito - G. Sichera, *L'informazione (e la disinformazione) nell'epoca di internet: un problema di libertà*, in *Costituzionalismo.it*, n. 1-2021.

va al fine di sopperire alle indubbi difficoltà di individuazione e raccolta delle prove di simili condotte "diffuse", poiché le fonti nazionali e comunitarie anche recenti hanno affrontato il problema dell'utilizzo "etico" e virtuoso dell'I.A. attraverso discipline e soluzioni di "soft law".

Tuttavia, i casi esaminati pongono indubbi problemi relativi alla necessità di disciplinare ed anche incriminare condotte che determinano eventi lesivi dei diritti fondamentali della persona o la sovranità dello Stato, proprio in tutti i casi in cui si pongano "al di fuori del contesto delle regole".

Ciò non appare risolvibile adeguatamente con la previsione di obblighi di controllo in capo ai gestori di piattaforme (siano persone fisiche o enti), non essendo esigibile sul piano costituzionale una responsabilità oggettiva "da posizione". Per converso, l'attribuzione a determinati soggetti (piattaforme social o autorità governative) di poteri e obblighi di repressione (o persino di prevenzione) rispetto al verificarsi di determinati illeciti – anche tramite interruzione delle condotte che condurrebbero al verificarsi dell'evento atteso – solleva essa stessa questioni di corretto bilanciamento degli interessi in gioco e di tutela di diritti costituzionalmente garantiti negli spazi virtuali, che non possono che rimanere prerogativa dello Stato e delle sue articolazioni.

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.

La vicenda Trump-Twitter è paradigmatica, non solo per il contenuto dell'inibizione, ma anche per il fatto che un ente privato si è arrogato la prerogativa di intercludere ad un singolo cittadino la possibilità di utilizzo uno strumento essenziale per esprimere la propria libertà comunicativa, che è oramai riconosciuto come un diritto fondamentale.

7. Conclusioni e proposte

È chiaro che uno Stato democratico – lungi dall'abdicare dal proprio ruolo – non può né rimanere inerte di fronte ai crimini realizzati in rete, né d'altro canto rischiare che la libertà di espressione rischi di essere in certi casi arbitrariamente o erroneamente limitata.

Pertanto, come proposto da buona parte degli autori e studiosi del fe-

nomeno, la via maestra è quella di un regolamento UE vincolante o di un accordo internazionale, anche se ridotto al minimo in quanto relativo alle sole finalità degli algoritmi, volto ad indirizzare l'utilizzo degli stessi secondo i valori costituzionali europei, secondo quello che viene definito in ambito anglosassone un «*Algorythm Constitutional by Design*». Occorre comunque una disciplina che attribuisca centralità al momento giurisdizionale: 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.

Occorre tornare ai Lavori dell'Assemblea costituente nel marzo del 1947 sui limiti della libertà di espressione: "Dobbiamo difendere la libertà e la democrazia".

Se l'intimo pensiero di alcuno oggi si manifesta in forme patologiche o addirittura criminali, contro queste manifestazioni patologiche e criminali, contro qualsiasi attentato al regime di libertà e di democrazia che noi intendiamo fondare su basi salde, e proprio perché vogliamo fondarlo su basi salde, la Repubblica deve reagire con la repressione punitiva, affidata all'autorità giudiziaria, e non con sistemi polizieschi, che si risolverebbero in una compressione della libertà e in una negazione della democrazia.

Bibliografia

19/5/2021 Reports on February actions – Fighting Covid-19 Disinformation Monitoring Programme | Shaping Europe's digital future, in *https://digital-strategy.ec.europa.eu/en/library/reports-february-actions-fighting-covid-19-disinformation-monitoring-programme*

2020 Joint report di Europol, United Nations Interregional Crime and Justice Research Institute (UNICRI) and Trend Micro EC3, p. 52

Allcott H. - Gentzkow M., *Social media and fake news in the 2016 Election*, in *Journal of Economic Perspectives*, n. 2/2017, pp. 213-214

Asaro P., *Determinism, machine agency, and responsibility*, in *Politica & Società*, Il Mulino, Bologna, 2014

Basile F., *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Diritto Penale e Uomo*, Milano, 2019

Bassini M. - Liguori L. - Pollicino O., *Sistemi di intelligenza artificiale, responsabilità e accountability. Verso nuovi paradigmi?*, collana in F. Pizzetti (a cura di), 2018

Bateman J., *Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios*, luglio 2020

Beck S., *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, p. 227 ss.

Blakkarly J., *A gay sex tape is threatening to end the political careers of two men in Malaysia*, SBS News, 17 giugno 2019

Breland A., *The Bizarre and Terrifying Case of the "Deepfake" Video that Helped Bring an African Nation to the Brink*, Mother Jones, 15 marzo 2019 (accesso 11 novembre 2021)

Brundage M. et al., *Malicious Use of Artificial Intelligence - MUAI*, 2008

Buscema L., *Reati elettorali e principio di democraticità dell'ordinamento: profili assiologici e ricostruttivi*; in *Diritto Penale Contemporaneo*, 28.10.2013

Cappellini A., *Machina delinquere non potest? Brevi appunti su intelligenza artificiale e responsabilità penale*, in *Criminalia*, 2019

Chesney R. - Citron D.K., *Deep Fakes: a looming challenge for privacy, democracy, and national security*, 2019, 107 California Law Review 1753, 1760

Coronavirus vaccine disinformation: new reports from online platforms to inform Code of Practice revamp, in *https://digital-strategy.ec.europa.eu/en/news/coronavirus-vaccine-disinformation-new-reports-online-platforms-inform-code-practice-revamp*

Corte Cost., sent. 10 luglio 1974, n. 225, in *Giurisprudenza costituzionale*, 1974, pp. 1775 ss.

Corte Cost., sent. 15 giugno 1972, n. 105, in *Giurisprudenza costituzionale*, 1972, pp. 1196 ss.

Cull N. J. - Culbert D.H. - Welch D., *Disinformation*, in *Propaganda and Mass Persuasion: A Historical Encyclopedia, 1500 to the Present*, ABC-CLIO, 2003, p. 104, ISBN 979-1576078203

Cuniberti M., *Il contrasto alla disinformazione in rete tra logiche del mercato e (vecchie e nuove) velleità di controllo*, in *MediaLaws*, n. 1/2017, p. 30

Di Biasi F. - Javadi M.: *A pro-Russian bot network in the EU amplifies disinformation about the war in Ukraine*, in *https://edmo.eu/reports*, April 28, 2022;

Dolhansky B. - Bitton J. - Pflaum B. - Lu J. - Howes R. - Wang M. - Canton F.C., *The DeepFake Detection Challenge (DFDC) Dataset*, in *https://arxiv.org/abs/2006.07397?fbclid=IwAR1n3A8Gr1Ldo8ojXw6ggzX0c*

CKOHKLD-jri5ZEHCSCJKNi4xoXaZCiqkNQ

Doncieux S. - Mouret J., *Beyond black-box optimization: a review of selective pressures for evolutionary robotics*, in *Evolutionary Intelligence*, 7, 2014, p. 71 ss.

European Digital Media Observatory, *V.D.D: Report on main trends and legal developments at national level on disinformation and national policies during the electoral campaigns / Policies to tackle disinformation in EU member States*, Reports - EDMO, in *https://edmo.eu/reports*

European Parliament Press Releases _ Plenary Session Juri, *Guidelines for military and non-military use of Artificial Intelligence*, 20.1.2021

Fiocca M., *Cyberterrorismo: le implicazioni dell'uso nocivo dell'intelligenza artificiale*, in *State Of Mind - Il Giornale delle scienze psicologiche*, 6 aprile 2021

Freitas P. - Andrade F. - Novais P., *Criminal Liability of Autonomous Agents: from the Unthinkable to the Plausible*, in P. Canovas - U. Pagallo - M. Palmirani - G. Sartor, *AI approaches to the Complexity of Legal System*, Springer, 2013

Goodfellow I.J. et al., *Generative Adversarial Networks*, 2014, arXiv:1406.2661 (accesso 11 novembre 2021)

Gross L., *A broken trust: lessons from the vaccine - autism wars*, in *PLoS Biol*, vol. 7, n. 5, 2009, pp. 756-9, DOI:10.1371/journal.pbio.1000114, PMC 2682483, PMID 19478850

Harwell D., *'Sexist' videos edited to make Nancy Pelosi look drunk go viral, with Trump's help*, in *The Independent*, 24 maggio 2019

Holmes A., *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, in *https://www.businessinsider.com/facebook-just-banned-deepfakes-but-the-policy-has-loopholes-2020-1?IR=T* (accesso 11 novembre 2021)

Http://www.unicri.it/News/Algorithms-Terrorism-Malicious-Use-Artificial-Intelligence-Terrorist-Purposes

Https://blog.youtube/news-and-events/how-youtube-supports-elections (accesso 11 novembre 2021)

Https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52021PC0206

Https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52021PC0206&from=IT (accesso 15 novembre 2021)

Https://help.twitter.com/en/rules-and-policies/manipulated-media (accesso 11 novembre 2021)

Https://www.europarl.europa.eu/doceo/document/TA-9-2021-0009_IT.html

(accesso 15 novembre 2021)
Https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_IT.html (accesso 15 novembre 2021)
Https://www.europol.europa.eu/publications-documents/malicious-uses-and-abuses-of-artificial-intelligence
Https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9512278 (accesso 11 novembre 2021)
Https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9512278
Mazzanti M., *Reati elettorali*, (voce), in *Enc. Dir*., XIV vol., Milano, 1965, 794-806. Cfr. anche F. Goisis, *Pretesa sostanziale del cittadino elettore nel contenzioso elettorale*, cit., 157.
Mervosh S., *Distorted Videos of Nancy Pelosi Spread on Facebook and Twitter, Helped by Trump*, in *The New York Times*, 24 maggio 2019
Monje Jr. C., *Twitter letter to Chairman Schiff*, su *Twitter*, 31 luglio 2019
Nagni E., *Artificial Intelligence, l'innovativo rapporto di (In)compatibilità fra machina sapiens e processo penale*, in *Sistema Penale*, fasc. 7/21, ISSN 2704-8098
Perrone R., *Fake news e libertà di manifestazione del pensiero*, in *Nomos*, n. 2/2018
Sammito F. - Sichera G., *L'informazione (e la disinformazione) nell'epoca di internet: un problema di libertà*, in *Costituzionalismo.it*, *n. 1-2021*, ISSN 2036-6744
Scott E.C., *Evolution vs. Creationism: An Introduction* (PDF), Second, Westport, CT, Greenwood Press, 2009, ISBN 9780313344275, su *cdn.who.int* (consultato il 1º novembre 2017)
Senn A., *Open Systems for Better Business: Something Ventured, Something Gained*, Van Nostrand Reinhold, 1995, p. 25, ISBN 978-0-442-01911-2
Spivak R., *"Deepfakes": The Newest Way To Commit One Of The Oldest Crimes*, Georgetown Law Technology Review; cite as: 3 geo. l. tech. rev. 339 (2019)
Westerlund M., *The Emergence of Deepfake Technology: A Review*, Technology Innovation Management Review, November 2019, Issue 11

Intelligenza artificiale, influenza sul mercato politico e reati contro la personalità dello stato. La prospettiva internazionalistica

di Massimiliano Signoretti*

Vorrei anzitutto ringraziare il Direttore della Scuola di Perfezionamento Forze di Polizia Generale la Gala per il graditissimo invito, sua eccellenza il Procuratore Generale dr. Salvi e la Fondazione Occorsio, per questa straordinaria opportunità di approfondimento di temi estremamente complessi e di attualità.

La prospettiva che si offre, in merito al tema dell'odierna conferenza, è una prospettiva internazionalistica. Pertanto, il punto di vista e il focus del presente intervento è quello dell'attività degli Stati nello spazio cyber. La questione che anzitutto si pone è se il diritto internazionale vigente risulti applicabile alle operazioni cyber condotte da uno Stato e dirette ad interferire con una delle fondamentali espressioni dei processi democratici degli Stati: i processi elettorali. E ciò anche nel caso i cui tali operazioni di interferenza siano condotte con sistemi di intelligenza artificiale. La successiva questione che si pone attiene alle circostanze in cui tali interferenze nei processi elettorali condotte con mezzi cyber possano essere considerate una violazione del diritto internazionale.

Casi paradigmatici per la nostra analisi sono le elezioni presidenziali statunitensi del 2016 e 2020. Tuttavia, trattandosi di un fenomeno globale, anche le elezioni in altri Paesi hanno sofferto simili tentativi (Italia, Francia, Ucraina e l'elenco potrebbe continuare). Possiamo, ad esempio, ricordare i tentativi di incendiare il dibattito sull'indipendenza della Catalogna, la Brexit. Ma anche gli incidenti cibernetici sofferti dalla stessa Russia, con gli "attacchi" DDOS del 2018 alla Commissione Elettorale Centrale.

In tema di interferenze nel processo elettorale di un Paese condotte attraverso il cyberspace, è utile distinguere tra operazioni dirette ad alterare aspetti tecnici del processo di voto e, di conseguenza, il risultato finale delle elezioni (dalla registrazione dei votanti, all'espressione del voto, dalla conta dei voti, alla raccolta dei risultati) e c.d. operazioni di mera influenza (*influence operations*), che mirino ad influenzare la campagna elettorale dei candidati e la percezione degli elettori (sia in merito ai candidati stessi, che in merito

(*) Tenente Colonnello dell'Aeronautica Militare italiana, Consulente Giuridico presso il Comando Interforze per le Operazioni in Rete e già ricercatore presso il NATO Cooperative Cyber Defence Centre of Excellence di Tallinn (Estonia) dal 2018 al 2021.

a determinati temi della campagna elettorale). Questo secondo tipo di operazioni cyber – che recano un evidente tentativo di influenzare il processo elettorale – hanno sicuramente caratterizzato le citate elezioni presidenziali USA del 2016 e del 2020. Le operazioni di influenza online in questi casi hanno infatti mirato sia ad alterare la percezione pubblica dei candidati, attraverso campagne di denigrazione di un candidato per favorirne un altro, sia a minare la fiducia nel processo elettorale e ad esacerbare le divisioni sociopolitiche all'interno del Paese. Per contro, tali campagne non hanno comportato anche il tentativo di alterare aspetti tecnici del processo di voto, quali l'amministrazione delle elezioni (ad esempio la registrazione dei votanti, l'espressione del voto in sé o il risultato del voto stesso). La distinzione non è fine a se stessa, poiché nell'un caso o nell'altro diverse sono le norme del diritto internazionale potenzialmente violate.

La questione è se l'interferenza elettorale condotta da uno Stato straniero nella dimensione cyber costituisca o meno un atto illecito internazionale. L'analisi, pertanto, da un punto di vista di relazioni tra gli Stati, richiede l'individuazione della specifica norma del diritto internazionale che si assume violata da tale condotta.

Per sgomberare il campo da eventuali equivoci, diciamo subito che nonostante spesso nel linguaggio comune ci si riferisca a tali attività come ad "attacchi cyber" in ambito NATO tali operazioni verrebbero probabilmente definite "sottosoglia" (*below the treshold*) e cioè al di sotto della soglia per cui un'operazione cyber sia di entità e con conseguenze tali da essere equiparata ad un attacco armato e quindi da implicare il ricorso alla legittima difesa ai sensi dell'articolo 51 della Carta delle Nazioni Unite e quindi all'uso della forza armata. Ciò nondimeno, tali operazioni possono costituire un illecito internazionale dello Stato.

Come è noto, infatti, il regime generale di responsabilità internazionale degli Stati è disciplinato da regole di diritto internazionale consuetudinario, oggetto di una codificazione a cura della Commissione di Diritto Internazionale delle Nazioni Unite che riproduce in prevalenza tali principi con alcuni aspetti evolutivi (gli Articoli sulla Responsabilità degli Stati per Atti Illeciti Internazionali). L'art. 1 della codificazione stabilisce che ogni atto internazionalmente illecito di uno Stato comporta la responsabilità internazionale di tale Stato. L'articolo 2, a sua volta, stabilisce che si è in presenza di un atto internazionalmente illecito di uno Stato quando una condotta consistente in un'azione o in un'omissione: (a) è imputabile allo Stato in base al diritto internazionale e (b) costituisce una violazione di un obbligo internazionale dello Stato. Questi sono i due elementi (il primo soggettivo ed il secondo

oggettivo) della responsabilità internazionale degli Stati. In base all'elemento soggettivo, pertanto, è necessario che vi sia un'azione od omissione giuridicamente attribuibile allo Stato e, in base all'elemento oggettivo, è necessario che vi sia una violazione di un'obbligazione (derivante da norme consuetudinarie o pattizie) che lo Stato ha verso un altro Stato. Venendo al caso dell'interferenza nelle elezioni, perché vi sia un illecito internazionale è anzitutto necessaria un'attribuzione legale (e non solo tecnica) della condotta illecita allo Stato. L'attribuzione legale denota una situazione in cui la condotta di un individuo o gruppo è considerata come azione dello Stato. Il problema, con particolare riguardo alle operazioni condotte con mezzi cyber, è rappresentato dalla varietà delle forme di relazione tra individui e Stati (organi, c.d. proxies, contractors, trolls, ecc.). La base giuridica del processo di attribuzione a uno Stato di operazioni di influenza elettorale condotta nel cyberspace è quindi e comunque rappresentata dall'esistenza di un rapporto organico tra l'agente e lo Stato (come affermato dagli Stati Uniti nel caso delle interferenze nelle elezioni presidenziali) o da un rapporto di direzione e controllo che uno Stato esercita sugli individui o gruppi (ad esempio, un rapporto contrattuale con un'agenzia di marketing o di consulenza) tale da poter concludere che l'operazione di influenza elettorale condotta attraverso le reti possa essere considerata come atto dello Stato (Articoli sulla Responsabilità Internazionale degli Stati, articoli da 4 a 8).

Evidentemente, non sempre il rapporto tra lo Stato e l'attore è chiaro e spesso l'attribuzione di un'operazione da un punto di vista tecnico può risultare estremamente complessa, ancor più quando l'operazione di interferenza è condotta attraverso l'impiego dell'intelligenza artificiale. Questo è il motivo per cui, a livello internazionale, l'attribuzione di una condotta ad uno Stato nello spazio cibernetico internazionale si fonda normalmente su uno standard della prova diverso (e generalmente attenuato) da quello normalmente richiesto nelle procedure giudiziarie del diritto nazionale. Lo standard applicato è infatti in questo caso quello della ragionevolezza (*reasonablness* o *high confidence*). Pertanto, in assenza di attribuzione (per impossibilità giuridica o tecnica di attribuire la condotta ad uno Stato) l'interferenza realizzata con capacità cibernetiche non costituirà una violazione del diritto internazionale.

Laddove, invece, vi siano evidenze della riferibilità della condotta allo Stato, l'ulteriore elemento da verificare per accertare l'esistenza di un atto internazionalmente illecito e quindi la responsabilità dello Stato è verificare se l'attività di interferenza nelle elezioni costituisca di per sé una violazione di una norma di diritto internazionale (elemento oggettivo). Solo in questo caso, infatti, la condotta attribuibile allo Stato potrà qualificarsi come illecito

internazionale e implicare la responsabilità internazionale di quello Stato. A tal proposito, è necessario individuare nel sistema di diritto internazionale una norma primaria (che cioè genera un obbligo di fare o di non fare nella relazione tra gli Stati) – di natura consuetudinaria o pattizia – di cui si assuma la violazione attraverso l'operazione condotta dallo Stato con mezzi cibernetici.

Anticipiamo sin da subito che le norme del diritto internazionale che più probabilmente sono suscettibili di essere violate da un'attività di interferenza nel processo elettorale di un altro Stato sono il divieto di intervento negli affari interni (o esterni) di un altro Stato, il principio di sovranità, i diritti umani. Come è noto, per affari interni o esterni di uno Stato si intende il c.d. *domain reservé*, cioè quella sfera di attività statale (pur soggetta ad un procedimento di progressiva erosione ad opera in particolare dei diritti umani) che il diritto internazionale lascia all'attività di regolazione degli Stati stessi (dove essi sono liberi di esercitare scelte discrezionali). Il divieto di intervento nel *domain reservé* è un principio di diritto internazionale consuetudinario, già riconosciuto dal Gruppo di Esperti Governativi delle Nazioni Unite nel 2015 a proposito delle operazioni cyber. Come chiarito nella decisone della Corte Internazionale di Giustizia nel caso Nicaragua contro Stati Uniti del 1986, un'attività di uno Stato, per costituire violazione del principio di non intervento, deve possedere due requisiti: il primo, essere diretta contro o avere ad oggetto il *domain reservé* di un altro Stato; e, secondo elemento, avere natura coercitiva. Chiarito cosa si intenda per *domain reservé*, vediamo più in particolare l'elemento della coercizione. Un'attività di uno Stato nei confronti di un altro è coercitiva quando priva uno Stato della libertà di decidere liberamente su questioni sovrane che il principio di sovranità affida esclusivamente allo Stato. Lo svolgimento del processo elettorale è certamente un esempio di attività afferenti al *domain reservé*. Nella citata decisione della Corte Internazionale di Giustizia, infatti, è chiarito come rientri sicuramente in questa sfera la "scelta del sistema politico". Laddove uno Stato – per le interferenze esercitate da un Paese straniero – sia costretto ad intraprendere un corso d'azione diverso da quello che lo stesso avrebbe liberamente scelto, allora le attività di influenza o i tentativi di persuasione (consentiti) divengono intervento, proibito in base al diritto internazionale.

Un approccio utile in questo senso, è distinguere quelle operazioni di influenza sul "mercato politico" condotte con attività informatiche che si dirigono verso la stessa amministrazione delle elezioni da parte dello Stato, o verso le infrastrutture elettorali o verso la possibilità degli elettori di esprime il voto. Un'ipotesi potrebbe essere quella di operazioni cyber il cui effetto sia l'alterazione del calcolo dei voti o il blocco delle procedure online di *e-voting* (si pensi al caso emblematico dell'Estonia dove già nel 2019 il 43.8% dei voti

è stato espresso con voto elettronico). Operazioni di soppressione del voto che abbiano come bersaglio i votanti possono assumere varie forme: ad esempio, la diffusione tramite social media di un falso incidente nelle vicinanze di un seggio elettorale, tale da disincentivare l'accesso al seggio; erronee istruzioni per l'espressione del voto diffuse online, che intenzionalmente alterino le indicazioni sulle modalità di voto elettronico o che forniscano informazioni fuorvianti sulla collocazione del seggio; ma anche la manipolazione dei sondaggi, suscettibile di disincentivare l'afflusso alle urne.

Altre operazioni cyber possono altrimenti essere dirette verso l'atteggiamento di voto degli elettori: si parlerà più precisamente in questo caso di operazioni di influenza. Dirette certamente agli elettori, ma il cui ultimo obiettivo è lo Stato. Potrebbe trattarsi di operazioni nel cyberspace che privino l'elettorato di informazioni elettorali, o dell'accesso a informazioni credibili sui candidati o su determinati temi della campagna elettorale. Si pensi ad esempio a DDOS (*Distributed Denial of Services*) su social media o sui media outlet di un partito; alla generazione di *fake user profiles* tramite agenti di Intelligenza Artificiale (fotografie, nomi, websites falsi) dedicati a campagne sistematiche di discredito di un candidato (*negative buzz*), allo sfruttamento delle divisioni sociali, al *dog whistling*.

Il semplice fatto di influenzare lo Stato preso di mira mediante la persuasione o la propaganda senza obiettivo e intento specifico di alterare l'esito del voto, non è sufficiente per qualificare l'interferenza elettorale come coercizione. L'elemento della coercizione comporta anche l'esigenza dell'intento diretto ad ottenere effetti distorsivi del voto. E a tal proposito è anche necessario un nesso causale tra l'atto coercitivo e l'effetto sugli affari interni o esterni dello Stato vittima.

La diffusione di "fatti alternativi" di per sé non costituisce una violazione della sovranità dello Stato: la propaganda, in altri termini, non interferisce in via diretta con le funzioni intrinseche del Governo e viene normalmente considerata nell'ambito dei diritti umani come forma di libertà di opinione e di espressione.

Diversamente, il tentativo di uno Stato straniero di promuovere l'elezione di un determinato candidato, la predisposizione di ingenti risorse finanziarie in suo favore, il riempimento o l'egemonizzazione dello spazio informativo con una campagna online a favore di un candidato, andrà valutato in base alle circostanze (ad esempio, se si tratti di elezioni municipali o statali) e agli effetti che tale campagna è in grado di produrre (ad esempio, l'elezione del candidato "gradito").

Poi c'è il tema della veridicità o falsità delle informazioni diffuse: può

parlarsi di intervento coercitivo in caso di diffusione di informazioni veritiere, laddove, almeno in principio, ciò dovrebbe concorrere ad una maggiore informazione e partecipazione consapevole degli elettori? Le questioni che si aprono sono diverse e di difficile soluzione. Si pensi al caso di egemonia dello spazio informativo, a notizie trafugate, e successivamente abilmente diffuse, in grado di dirottare i voti degli elettori. La consapevolezza da parte degli elettori che i dati diffusi rappresentano il frutto di un trafugamento o sottrazione operato da uno Stato estero cambierebbe il loro atteggiamento nei confronti di quei dati? Se esiste una presunzione che la diffusione di informazioni veritiere non violi in principio il diritto internazionale in quanto esercizio del diritto all'informazione (si pensi alle elezioni statunitensi del 2016 e alla diffusione delle e-mail del Comitato Democratico Nazionale[1]), sorge anche legittima la questione se la consapevolezza da parte degli elettori che i dati diffusi rappresentano il frutto di un trafugamento o sottrazione operato da uno Stato estero cambierebbe il loro atteggiamento nei confronti di quei dati.

Altra norma (o principio) di diritto internazionale che è suscettibile di essere violato da operazioni cyber di interferenza nella campagna elettorale di un altro Stato è il principio di sovranità. Il contenuto di questo principio di diritto consuetudinario – i cui capisaldi si trovano anche negli articoli 1 e 2(4) della Carta delle Nazioni Unite e che implica la necessità nelle relazioni tra Stati di rispettare la sovranità di un altro Stato – è stato descritto in una decisione della Corte Permanente di Arbitrato (Isola di Palmas, 1928), in cui, in breve, la Corte descriveva la sovranità di uno Stato come il suo diritto di esercitare in un designato territorio le funzioni proprie dello Stato. La violazione di tale principio del diritto internazionale, nel caso di interferenza nel processo elettorale condotto con operazioni cyber (usando o meno algoritmi di intelligenza artificiale), può avvenire anzitutto con una violazione dell'integrità territoriale dello Stato. Si pensi all'ipotesi di un'operazione condotta con mezzi informatici che provochi un danno fisico con conseguenze materiali in un altro Stato ovvero – anche se questo è un aspetto dibattuto – un danno dalla perdita di funzionalità di taluni sistemi per un periodo di tempo determinato (come ad esempio la compromissione della funzionalità di strutture elettorali). Si pensi, in questo senso, alle operazioni di DDOS condotte nei confronti dell'Ucraina nel 2014. Da notare che taluni Paesi (la Francia, in particolare) ritengono che ogni accesso non autorizzato ai sistemi digitali nazionali condotto da un Paese straniero rappresenti una violazione della propria sovranità nazionale.

1) Il *Democratic National Committee* (DNC) è l'organo di Governo del Partito democratico degli Stati Uniti. Il comitato coordina la strategia per supportare i candidati del Partito Democratico in tutto il Paese per cariche locali, statali e nazionali.

Ma la violazione del principio di sovranità può altresì avvenire, attraverso un'interferenza nei sistemi informatici (anche) elettorali che si sostanzi in una usurpazione di funzioni governative sovrane. E a questo proposito non è necessario che si tratti di interferenza di tipo coercitivo (intervento), né che da tale interferenza derivino effetti fisici o di perdita di funzionalità, come nel caso della violazione dell'integrità territoriale. L'atto di interferenza è di per sé sufficiente a determinare la violazione del principio di sovranità, atteso che tale tipo di interferenza ha ad oggetto funzioni sovrane dello Stato (lo svolgimento del processo elettorale). Così nel caso di interferenza con le infrastrutture informatiche di gestione delle elezioni, il blocco dell'accesso ad informazioni elettorali, o la manipolazione di informazioni attinenti alle elezioni, costituirebbe violazione della sovranità dello Stato vittima.

Le operazioni cyber sullo svolgimento del processo elettorale possono altresì coinvolgere taluni diritti umani. Su questo tema si innesta un complesso dibattito circa l'applicabilità extraterritoriale di tali diritti, che tuttavia non è possibile affrontare in questa sede. Può però affermarsi che esiste un generale consenso circa un obbligo generalizzato per gli Stati di rispetto dei diritti umani così *offline* come *online*. Tra i diritti umani che vengono particolarmente in rilievo nella sfera digitale vi è, anzitutto, il diritto alla libertà di espressione (diritto a ricercare, ricevere e fornire informazione al di là delle frontiere statuali). Il riconoscimento di tale diritto giustificherebbe l'interferenza di uno Stato nel processo elettorale di un altro Stato (che ad esempio, per finalità politiche, ostacoli la diffusione di determinate informazioni al suo interno). Da un punto di vista statistico, è assai più probabile che sia lo Stato che conduce l'elezione a limitarli (obblighi imposti a Internet Service Providers o social media di filtrare i contenuti trasmessi da altri Stati), piuttosto che uno Stato dall'esterno. Il diritto alla privacy o riservatezza, altresì di estremo rilievo nella sfera digitale, è riconosciuto come diritto consuetudinario (come quello di espressione) ed è oggetto di riconoscimento in varie convenzioni internazionali (ad esempio nella Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, articolo 8). Va in ogni caso ricordato come tali diritti non siano considerati come diritti assoluti, potendo lo Stato eccezionalmente limitarli. per scopi legittimi e in modo ragionevole.

Un altro argomento di rilievo per il tema oggetto della discussione è quello del c.d. spionaggio informatico. Lo spionaggio (o attività di intelligence) in tempo di pace è stato tradizionalmente considerato non regolamentato dal diritto internazionale e, come, tale non considerato come condotta illecita nelle relazioni tra Stati. Ciò è riconosciuto anche nel Manuale di Tallinn 2.0, in cui si afferma che "sebbene lo spionaggio informatico in tempo di pace

da parte degli Stati non violi di per sé il diritto internazionale, il metodo con cui viene effettuato potrebbe costituirne una violazione". Si deve rilevare, tuttavia, che per quanto le operazioni di spionaggio informatico non siano generalmente illegali dal punto di vista del diritto internazionale, di solito sono vietate e oggetto di previsione criminale secondo il diritto interno degli Stati.

La citata sottrazione e successiva pubblicazione delle e-mail private dei componenti del team della campagna elettorale di un candidato del Comitato Nazionale Democratico (DNC) in occasione delle presidenziali USA del 2016, può certamente essere considerata un'operazione di spionaggio diretta ad influenzare la campagna elettorale degli Stati Uniti, come è stato successivamente accertato dalle successive indagini. A tale riguardo il diritto internazionale – che generalmente non sarebbe violato da una simile condotta in quanto non esiste una norma che vieta lo spionaggio a livello internazionale – potrebbe tuttavia risultare violato in considerazione delle modalità con cui tale operazione è stata effettuata. Laddove l'operazione di esfiltrazione delle e-mail dei membri del DNC si fosse realizzata attraverso un'operazione di c.d. "accesso ravvicinato", ovvero inviando fisicamente degli operativi sul suolo statunitense per procedere alla sottrazione non autorizzata di dati confidenziali dal server target, la lesione (o *breach*) del diritto internazionale sarebbe costituita dalla violazione del principio di sovranità territoriale del Paese. Diversamente, facendo un'altra ipotesi, un'operazione di cyber spionaggio preordinata al successivo sabotaggio del sistema di scrutinio elettronico del voto costituirebbe, con ogni probabilità, un'usurpazione di funzioni intrinsecamente sovrane o governative, e, come tale, un illecito internazionale, in quanto integrante una violazione della sovranità dello Stato o persino un intervento negli affari interni dello Stato stesso.

Un illecito internazionale può essere costituito sia dalla violazione di un obbligo di non fare (come nel caso della violazione della regola della sovranità statale attraverso un'operazione informatica che interferisca direttamente nel processo elettorale), ma anche dalla violazione di un obbligo di fare. Questa seconda ipotesi ricorre nei casi in cui uno Stato sia in violazione del c.d. dovere di *due diligence*, in base al quale gli Stati hanno l'obbligo di agire adottando ogni misura percorribile nei confronti di un'operazione cyber che promani dal proprio territorio e che realizzi una lesione di diritti di altri Stati[2]. Trasposto nel tema della nostra discussione, in base a tale principio uno Stato ha l'obbligo di porre termine all'interferenza nelle elezioni di un altro Stato che promani da infrastrutture cyber situate sul proprio territorio, anche se condotte da remoto da

2) Il principio venne affermato dalla Corte Internazionale di Giustizia nel caso del Canale di Corfù del 1949 ove la Corte stabilì che uno Stato non deve consentire consapevolmente che il suo territorio venga usato per atti contrari ai diritti di altri Stati.

un Paese terzo. Laddove sia a conoscenza di tale attività ed ometta di adottare le misure possibili per porvi fine, tale Stato sarà considerato in violazione di tale dovere e quindi in violazione del diritto internazionale. Va tuttavia chiarito, a tal proposito, che a livello internazionale, almeno al momento, non esiste un consenso sulla natura consuetudinaria del principio.

Esaminati quali siano le norme del diritto internazionale potenzialmente suscettibili di essere lese da attività di interferenza nel processo elettorale condotte da Paesi stranieri, passiamo brevemente in rassegna le risposte che il sistema del diritto internazionale rende legalmente disponibili agli Stati che siano vittima di tali attività.

A livello internazionale, il paradigma reattivo che uno Stato ha a disposizione nei confronti di un'operazione cyber al di sotto della soglia dell'attacco armato che violi la propria sovranità è fornito dal citato diritto consuetudinario codificato a cura della Commissione di Diritto Internazionale delle Nazioni Unite negli articoli sulla Responsabilità Internazionale degli Stati per Atti Illeciti Internazionali del 2001. La gamma di misure in autotutela sono previste dall'ordinamento internazionale (capitolo V della codificazione, articoli 20-25, concepite e strutturate come circostanze escludenti l'illeceità della risposta dello Stato). Tali misure di reazione (o rimedi) disponibili in base al diritto internazionale vigente in caso di un'attività cyber malevola, possono essere di livello e intensità differente. Accennerò brevemente solo alle "ritorsioni" e alle "contromisure". Le prime sono misure di reazione che, per quanto non amichevoli, non violano il diritto internazionale e non costituiscono illecito. Ad esempio, l'espulsione dal territorio nazionale di diplomatici del Paese che si presume autore della violazione, l'adozione di sanzioni economiche, la chiusura di sedi consolari. Quella citata, dell'adozione di misure di ritorsione, è stata la via intrapresa dal Governo degli Stati Uniti a seguito dell'illecita interferenza nelle elezioni presidenziali del 2016. Considerato, come si è notato, che le ritorsioni non costituiscono di per sé atti illeciti, atti di ritorsione sono ammessi anche quando l'operazione di interferenza nelle elezioni non costituisca violazione del diritto internazionale, perciò anche in assenza di un illecito. E per questa ragione probabilmente sono le misure reattive più frequentemente adottate dagli Stati. Diversamente, le "contromisure" sono comportamenti in risposta al torto subito che violano a loro volta una norma di diritto internazionale, ma possono essere adottate da uno Stato vittima di un'attività cyber che costituisca essa stessa un illecito internazionale (ad esempio, attività di interferenza nel processo elettorale tali da costituire una violazione del principio di sovranità). Evidentemente, l'illecito iniziale (l'interferenza illecita nel processo elettorale), di cui le contromisure costi-

tuiscono 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 un altro Paese).

Con riferimento, infine, alla problematica della risposta giurisdizionale nazionale 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. A seguito delle interferenze nelle citate elezioni presidenziali del 2016, infatti, il Governo degli Stati Uniti, parallelamente alla risposta a livello del sistema sanzionatorio internazionale (ritorsioni) ha avviato procedimenti penali a carico dei (presunti) responsabili delle operazioni di interferenza nelle elezioni, che tuttavia, nell'impossibilità di estradare gli autori, ha rappresentato prevalentemente un messaggio di deterrenza (c.d. *namimg and shaming*).

Bibliografia

Autori Vari, *Autonomous Cyber Capabilities under International Law*, Ed. R. Liivoja, A. Väljataga NATO CCDCOE Publications, 2021

D. Broeders - B. Van den Berg, *Governing Cyberspace: Behaviour, Power and Diplomacy*, Pubblicazioni Rowman & Lttlefield, 2020.

G. Corn - R. Taylor, *Sovereignty in the Age of Cyber*, in *American Journal of International Law*, 2017

International Group of experts, *Tallinn Manual 2.0 on the international law applicable to cyber*, Cambridge University Press, 2017

M.N. Schmitt, *Foreign Cyber Interference in Elections*, in *International Law Studies*, vol. 97, Stockton Center for International Law, 2021

M.N. Schmitt, *Virtual Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law*, in *Chicago Journal of International Law*, Vol. 19, No. 1, Article 2, 2018

S. Watts, *Low-Intensity Cyber Operations and the Principle of Non-Intervention*, SSRN: *https://ssrn.com/abstract=2479609*, 2014

United Nations International Law Commission, *Responsibility of States for Internationally Wrongful Acts*, in *Yearbook of the International Law Commission*, 2001, Vol. II (Part Two)

Intelligenza artificiale, influenza sul mercato politico e reati contro la personalità dello Stato. La criminalità terroristica

di Maurizio Romanelli*

Il tema dei rapporti tra intelligenza artificiale e influenza sul mercato politico è particolarmente ampio; è quindi necessario operare alcune selezioni e procedere in prospettiva di sintesi e di semplificazione.

Atteso che viene chiesto di offrire anche dati di esperienza, preferisco concentrare l'attenzione sul mondo del terrorismo, prevalentemente internazionale, proponendo – in via di sintesi – alcune chiavi di lettura che nascono per l'appunto dall'esperienza, rinviando per analisi più sistematiche ad altri contributi[1].

L'esperienza sul mondo del terrorismo, e sul contrasto alle sue varie forme di manifestazione, può forse consentire di dare risposte ai due quesiti ormai quasi classici, intorno ai quali girano gli approfondimenti svolti in questa occasione di studio e di ricerca:

– l'Intelligenza Artificiale come strumento per la commissione di reati;

– l'Intelligenza Artificiale come (nuovo ed ulteriore) strumento di contrasto all'interno del sistema normativo dato.

Si tratta di due questioni che hanno rilevanza di carattere generale all'interno della macro-area dei rapporti tra intelligenza artificiale e sistema penale, ma che – ovviamente – assumono un rilievo del tutto peculiare rispetto ai fenomeni del terrorismo.

Porto innanzitutto l'attenzione – all'interno dei limiti già indicati – sulla prima questione.

Vorrei cominciare offrendo in prima battuta dati di esperienza sulla realtà empirico-criminologica del terrorismo internazionale, quale si è manifestato a fare corso dalla data simbolo dell'11 settembre 2001 per circa un ventennio, passando dal tempo di Al Qaida all'affermazione di Islamic State, e poi nei diversi periodi di I.S.[2], sino alla sconfitta sul campo, ed all'attuale,

(*) Procuratore Aggiunto della Procura della Repubblica presso il Tribunale di Milano.

1) Rinvio a C.O. Onorati, *I.A., politica e reati contro la personalità dello Stato*, in *Sistema penale*, 13 giugno 2022, all'interno della raccolta degli atti del workshop della Fondazione Occorsio su *Intelligenza artificiale e giurisdizione penale.* Più in generale, su questioni classiche in tema di rapporti tra intelligenza artificiale e sistema penale, rinvio a F. Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Diritto penale contemporaneo*, 29 settembre 2019.

2) Per una possibile individuazione di *periodi* all'interno dell'operatività dello Stato Islamico, e per la ricostruzione dei *relativi fenomeni criminali*, rinvio – per chi fosse interessato – a M. Romanel-

quasi completa, scomparsa del c.d. terrorismo territoriale.

È ampiamente noto che si è trattato di un periodo terribile per una pluralità di Stati, europei ed extraeuropei, che hanno dovuto fare i conti – tutti – con la nuova realtà criminale e con le connesse esigenze di prevenzione/contrasto, attraverso il progressivo adeguamento della legislazione complessiva (non solo penale, ma anche processuale, ordinamentale, relativa alle agenzie di informazione, ecc.) e delle relative prassi di contrasto.

Do per acquisite, in questa sede, le conoscenze di base sull'evoluzione della nostra legislazione, a fare corso dall'immediato post torri gemelle, con il fondamentale d.l. n. 374 del 18 ottobre 2001, passando attraverso la riforma immediatamente successiva alla strage di Londra del 7 luglio 2005 (D.l. 144 del 27 luglio 2005) ed arrivando alla riforma successiva alla proclamazione di Islamic State ed alla ripresa degli attentati in Europa, soprattutto Parigi (D.l. n. 7 del 18 febbraio 2015).

Oggi ci troviamo di fronte ad una situazione in evoluzione, fluida, non facilmente decifrabile, sia per le caratteristiche evolutive del fenomeno criminale, che per il possibile "nuovo", determinato – appunto – tra le altre cose dall'evoluzione tecnologica.

Il "nuovo" è anche rappresentato dallo scoppio della pandemia da Covid-19, e dalla guerra di aggressione alle porte dell'Europa, due ulteriori fatti inimmaginabili, in aggiunta all'inimmaginabile rappresentato dall'attacco delle Torri Gemelle dell'11 settembre 2001.

Se è già molto complesso conoscere lo scenario e le linee evolutive del terrorismo c.d. islamico, la questione si complica ulteriormente se si porta l'attenzione sull'evoluzione del fenomeno del terrorismo su base suprematista, razzista, nazista, sulle sue reti, sui meccanismi di radicalizzazione e di passaggio all'azione, sui vari fronti e territori, soprattutto extraeuropei, ma con significative punte anche in Europa ed in Italia, come è purtroppo tristemente noto a partire dalla terribile strage di Utoya del 22 luglio 2011, fino alle gesta di Luca Traini del 3 gennaio 2018[3].

LI, *Criminalità organizzata e terrorismo: la circolazione dei modelli criminali e degli strumenti di contrasto*, in *Sistema penale*, 20 dicembre 2019.

3) Non mancano i precedenti significativi. Tra il giugno 2006 e l'aprile 2008 vi sono stati – tra Milano e provincia – oltre *una dozzina di attentati* a mezzo di molotov e di *pipe-bomb* in danno prevalentemente di luoghi di culto islamico, ma anche soltanto di luoghi legati al radicamento della comunità islamica in area milanese. Le indagini hanno consentito di chiarire che vi era un progetto puramente e semplicemente *antislamico*. Il gruppo responsabile delle azioni si firmava *Fronte Cristiano Combattente*, ed aveva l'obiettivo di contrastare *con tutti i mezzi* la presenza dei musulmani in Italia. Il principale autore degli attacchi ricostruiti, e anche di altri in via di programmazione, era Roberto Sandalo, ex terrorista di Prima Linea, poi diventato fondamentale collaboratore di giustizia nel contrasto al terrorismo interno, e confluito infine su posizioni anti-islamiche tanto da operare come *Fronte Cristiano Combattente* per la lotta armata contro l'Islam ed i "*bastardi islamici*".

In un quadro di questo tipo, le questioni relative all'impiego dell'intelligenza artificiale rappresentano prevalentemente ancora la formulazione di ipotesi, da una parte, e dall'altra la valutazione della minaccia in prospettiva di capacity building sul piano sovranazionale ed interno.

Senza pretese di completezza, proverò a delineare alcuni possibili impieghi di I.A. nel settore dei delitti contro la personalità dello Stato, e poi provo a ragionare sui relativi scenari.

La premessa necessaria è che il terrorismo c.d. islamico ha dimostrato ottima capacità di governo della tecnologia avanzata, soprattutto della rete internet e dei social media, utilizzandoli con qualità crescenti nel passaggio da Al Qaida ad Islamic State.

Questa "qualità" nella gestione delle tecnologie avanzate si è dimostrata essenziale rispetto ad alcune delle caratteristiche di fondo del terrorismo c.d. islamico e dei suoi fattori di forza: propaganda, arruolamento, addestramento ed autoaddestramento, radicalizzazione funzionale al passaggio all'azione, chiamata all'"egira"[4], rivendicazione di attentati e quindi ancora propaganda attraverso la rivendicazione, ecc.

Parallelamente l'evoluzione dei sistemi di intelligenza artificiale ha realizzato una maggiore accessibilità e facilità di uso degli stessi, e quindi anche una maggiore possibilità di forme di impiego.

Vi sono pertanto almeno due ragioni convergenti che impongono, o quanto meno giustificano, la domanda sul "che cosa succede quando il terrorismo governa ed impiega l'A.I.", oppure ancora sul "è A.I. il futuro del terrorismo?"; svolgeremo innanzitutto una serie di precisazioni, assolutamente necessarie, sia pure in prospettiva di sintesi.

Prima precisazione.

Si tratta, come sopra detto, prevalentemente di ipotesi di lavoro per adeguare le capacità di risposta degli Stati e della comunità internazionale rispetto ad una valutazione di rischio.

Ma è necessario sempre accompagnare la formulazione di ipotesi con dati di conoscenza empirica effettiva, parametrati sulla realtà delle forme di manifestazione del terrorismo, e con l'impiego – sempre – di strumenti inve-

4) La chiamata all'"egira" è l'*ordine* impartito da I.S. ad ogni "vero" musulmano di raggiungere il territorio dello Stato Islamico, abbandonando i territori della miscredenza: si tratta di un vero e proprio ordine, accompagnato dalla minaccia di pesanti conseguenze e sanzioni nel caso di inosservanza. È ovvio che la *hijra* è stata resa possibile, con imponenti fenomeni di emigrazione sia dall' Europa che da Paesi extraeuropei, nella misura *in cui vi fosse il territorio del Califfato*, e fin quando vi è stato. Numerose indagini svolte in Italia, attraverso la qualità dei nostri strumenti investigativi e l'esperienza delle nostre forze di Polizia, hanno dimostrato la centralità dell'ordine di raggiungere *Islamic State*, soprattutto nei primi mesi successivi alla proclamazione del Califfato da parte del "califfo" Abu Bakr Al-Baghdadi, e poi nei primi mesi del 2015.

stigativi/preventivi efficaci, che consentano la migliore conoscenza del fenomeno e la maggiore tempestività possibile nella risposta.

È questo un aspetto importante, del quale discuto da tempo, soprattutto per segnalare quanto la positiva esperienza del nostro Paese nel contrasto a gravi forme di criminalità, quali il terrorismo interno e le mafie, abbia consentito di affrontare con tempestività ed efficacia la sfida portata dal terrorismo internazionale (addirittura già ben prima delle Torri gemelle)[5].

La "paura del nuovo possibile" deve sempre accompagnarsi all'attenzione sui dati di realtà, e ogni vera investigazione – anche la più tecnologicamente avanzata – deve e dovrà accompagnarsi sempre con la migliore possibile conoscenza dei fenomeni territoriali, delle persone in carne ed ossa, delle ragioni delle scelte radicali, delle motivazioni profonde (anche quando non sono profonde le motivazioni ci sono in tema di terrorismo, e conoscerle è necessario in prospettiva di prevenzione ed anche – eventualmente – di "deradicalizzazione").

Ancora, sotto altro aspetto: la paura, ed ogni forma di narrazione allarmistica, in materie di così grande delicatezza, sono anche fattori di business per una molteplicità di soggetti privati, individui e società, e quindi anche di tentativi di influenza/condizionamento sul mondo dei decisori pubblici.

La paura è strumento da maneggiare con cautela, e con consapevolezza di tutti i significati, anche puramente economici.

Seconda precisazione.

Si tratta di un discorso estremamente complesso, al quale faccio solo cenno, che rappresenta la chiave di volta di qualunque seria capacità di risposta ai fenomeni del terrorismo, sia giudiziaria che sul piano della prevenzione/sicurezza.

Il terrorismo attuale (in tutte le sue forme di manifestazione) è sovranazionale, e quindi soltanto la cultura reale della condivisione delle informazioni, della circolazione delle stesse, del confronto spontaneo tra gli attori del contrasto operanti nei diversi Stati, in un quadro di fiducia reciproca, può consentire risposte efficaci e tempestive.

Su questo tema molto è stato fatto negli ultimi anni, e l'Italia ha portato straordinari dati di esperienza e di metodo; molto però rimane da fare, ed è bene che sia sempre segnalata questa esigenza di fondo.

Terza precisazione.

Quale che sia il livello di aggressione a beni fondamentali, individuali e collettivi, portati dal terrorismo, nelle sue varie forme di manifestazione ed

5) Per chi fosse interessato rinvio a M. Romanelli, *Riflessioni sul complessivo sistema di contrasto al terrorismo internazionale in Italia*, in *Diritto penale contemporaneo*, 14 giugno 2019.

– in ipotesi – oggi "armato" di A.I., solo una risposta legale e rispettosa dei diritti è al tempo stesso efficace.

Come ho avuto già modo di evidenziare in altre occasioni, valorizzando le caratteristiche di fondo del contrasto al terrorismo nell'ambito del nostro sistema penale costituzionale, la forza dello Stato viene dalle regole: qualunque cessione di quote di regole giova solo alla causa del terrorismo, divenendo straordinario fattore di radicalizzazione ai fini dell'azione terroristica.

Non sono affermazioni vuote di contenuto, ma dati di esperienza univoci.

Anche ragionando su ipotesi di nuove forme di aggressione, e di nuove "sfide", il sistema di contrasto dovrà continuare ad offrire queste caratteristiche di fondo e rispettare queste regole fondamentali.

Fatte queste premesse di metodo, è quindi del tutto corretto chiedersi quali sono le prospettive di impiego di A.I. da parte del terrorismo.

Semplificando, e seguendo le linee di approfondimento più aggiornate[6] a livello internazionale, le nuove minacce sono relative a tre macroaree:

– *cyber threats*;
– *psysical threats*;
– *political threats.*

Alcuni cenni a ciascuna delle tre aree ed alcune riflessioni possibili, oltre che dati di esperienza.

Cyber threats

I cyber attacks sono una realtà, ormai da numerosi anni; sono modalità di aggressione con potenzialità offensive enormi e sono stati effettivamente usati da Islamic State.

In tale settore, l'impiego dell'intelligenza artificiale appare tutto sommato semplice, e con capacità enorme di moltiplicazione dei risultati di offesa, soprattutto rispetto ad aggressioni abbastanza "basiche" quali quelle note come DoS o DDos.

6) Si veda l'ampio rapporto "*Algorithms and terrorism: the malicious use of artificial intelligence for terrorist purposes*", redatto congiuntamente dal *Counter Terrorism* delle Nazioni Unite (UNCCT) e dal corrispondente centro di ricerca (UNICRI) nel 2021. Il rapporto appare apprezzabile anche perché *non* enfatizza il livello della minaccia, ma anzi muove dalla premessa dell'assenza di prove significative in ordine all'effettivo impiego di A.I. da parte di gruppi terroristici: "*From the outset, it is important to clarify that no clear evidence of the actual use of A.I. by terrorist organizations has been identified by date*". È però opportuno ricordare anche che il mondo del terrorismo internazionale si è mosso nel corso degli anni arrivando all'"inimmaginabile" – basta pensare alle stragi dell'11 settembre 2001 – e che quindi "*a failure of imagination can have deadly consequences*" (rapporto cit., p. 26). Del resto, la Commissione d'inchiesta degli Stati Uniti sull'11 settembre ha concluso i suoi lavori segnalando espressamente che è *un limite* non avere *capacità di immaginazione* quando ci si confronta con l'agire terroristico sovranazionale, invitando così le agenzie di controllo ad "*istituzionalizzare l'immaginazione*".

Poco da dire – allo stato – sul piano del contrasto alla minaccia.

Si tratta di un classico problema di prevenzione/sicurezza, prima e più che di investigazione giudiziaria: le infrastrutture informatiche strategiche (economiche, militari, sistema di trasporti, salute, istruzione) devono avere livelli di protezione adeguati al livello della minaccia; la minaccia cresce e deve crescere la capacità di protezione.

Non molto dissimili le considerazioni di base in ordine ad altre note tipologie di aggressioni informatiche (malware; ransomware; man-in-the-middle, ecc.).

Non sembra che con riferimento a casi di questo tipo, destinati a crescere, siano possibili riflessioni ulteriori: si tratta di modalità di aggressione note, amplificate dalla capacità degli algoritmi di machine learning.

Certamente, le cose si complicano enormemente, con l'I.A. come aggressore e l'I.A. come difensore, o come aggressore di ritorno; ma dal punto di vista dei concetti di base, non mi sembra si vada oltre l'evidenziazione dell'esigenza di adeguata protezione/sicurezza.

Nella discussione orale ho ricordato un aspetto, peraltro noto, e cioè che l'impatto dell'aggressione informatica può consistere non solo nella distruzione – totale/parziale, duratura/limitata nel tempo – di un sistema informatico, ma anche nella esfiltrazione di dati rilevanti, con successivi impieghi criminali dei dati stessi.

Ve ne sono stati numerosi esempi.

Senza entrare nei dettagli, un'aggressione informatica di questo tipo fu quella indirizzata nel 2015 contro una delle società leader a livello mondiale nella produzione e vendita di sofisticata tecnologia informatica, anche a Paesi stranieri, con sede a Milano.

All'esito dell'attacco informatico venne effettuata, sulla rete, la pubblicazione molto rilevante di dati sensibili, compreso il codice sorgente relativo al più raffinato sistema di presa di controllo di telefoni cellulari del tempo, venduto ad una pluralità di società che a loro volta offrivano la propria tecnologia al servizio di indagini, anche della Procura della Repubblica di Milano oltre che di altre Procure Distrettuali.

Il risultato immediato fu l'interruzione delle attività di intercettazione telematica ed ambientale che erano in corso in più procedimenti per fatti di terrorismo internazionale.

Il 2005, come è ampiamente noto, fu uno degli anni in cui più preoccupante era la progettualità terroristica verso i Paesi occidentali, Italia compresa, e la Procura di Milano dovette chiudere da un giorno all'altro attività di intercettazione molto utili, e cambiare radicalmente i programmi del proprio

intervento, tra l'altro in un procedimento in cui il rischio di azione terroristica contro obiettivi situati all'interno dello Stato Italiano era molto elevato.

Cambiò anche – di conseguenza – il rapporto tra prevenzione/sicurezza ed esigenze investigative, argomento di grandissima rilevanza nelle "vere" indagini di terrorismo, con la definitiva prevalenza dell'esigenza di prevenzione.

Molto in sintesi: se la tecnologia non offre più adeguato controllo degli indagati e delle loro attività (h. 24, come si dice in gergo), allora ci vuole un intervento immediato, o in termini giudiziari (se ve ne sono i presupposti) o in termini amministrativi (espulsione dal territorio dello Stato).

La materia è delicatissima, richiede esperienza e formazione, ma non è possibile trattarla qui adeguatamente.

Psysical threats

C'è ampia letteratura sul tema, soprattutto in lingua inglese, ma non vi sono troppe riflessioni da svolgere.

È ovvio che l'A.I. può rappresentare uno strumento per la moltiplicazione degli attacchi e per la maggiore efficacia degli stessi.

Gli esempi abitualmente fatti riguardano, prevalentemente, i due settori dell'impiego di droni, e dell'impiego di autovetture a guida autonoma (senza conducente) attraverso la presa di controllo del sistema di guida.

Vi sono in realtà ipotesi di lavoro ancora più drammatiche.

Ancora una volta si tratta di ipotesi possibili, rispetto all'impiego dei droni già in parte realizzate, che aggiungono qualcosa al livello della minaccia, che è e rimane alta a prescindere dall'impiego di sistemi di intelligenza artificiale (l'ipotesi non appare oggi molto lontana da altre fatte in passato in un crescendo di allarmi non sempre giustificati, come ad es. l'ipotesi della presa di possesso di centrali atomiche da parte di gruppi di terroristi, o di aerei militari, ecc.).

Deve essere aggiunto e valutato un dato di esperienza, noto agli attori del mondo del terrorismo.

Uno dei vantaggi tradizionalmente segnalati in relazione all'ipotesi dell'uso di self-driving car – grazie all'impiego di A.I. – è la non necessità del rischio di sacrificio della propria vita nella conduzione dell'attacco, o, in alternativa, la non necessità del rischio di "cadere prigionieri" del nemico che si vuole abbattere.

Si tratta di vantaggi possibili e correttamente enunciati, ma è bene ricordare che i meccanismi di radicalizzazione, particolarmente efficaci attraverso una grande capacità di propaganda, fanno riferimento all'azione individuale ed al sacrificio, fino all'attacco suicida, come ad una delle massime realizza-

zioni dei doveri del combattente e quindi del "vero" musulmano.

Già nel periodo di formazione di Islamic State come terrorismo territoriale, e poi durante il periodo di Islamic State, l'attacco suicida ha rappresentato un valore, non un rischio: valore fortemente rivendicato e propagandato attraverso una vera e propria procedura di comunicazione particolarmente efficace e che rappresentava un fortissimo collante.

Nella fase nota di maggiore potenza di Islamic State il sacrificio della vita è una forza, non un rischio da evitare[7].

Questo non vuol dire che vi sia – o vi sarà – il rifiuto di mezzi aggressivi tecnologici che prescindano dal sacrificio della vita propria, ma solo per segnalare che la radicalizzazione è stata, ed è, centrale nell'affermarsi del jihadismo globale e passa attraverso il profondo coinvolgimento delle persone, in carne ed ossa, con il valore aggiunto del sacrificio della vita.

È certo però che uno spettacolare attacco realizzato attraverso la più avanzata tecnologia avrebbe quell'effetto di evidenza della propria forza, con connessa disseminazione della paura e del terrore, che rappresentano il mezzo dell'agire terroristico.

Political threats

L'argomento è oggetto di approfondimento in altra relazione e porto qui solo alcuni spunti utili al tema che tratto.

Il rischio di condizionamento della politica attraverso deep fakes è molto elevato sotto vari profili, e vi sono già stati esempi significativi in numerose parti del mondo, anche se forse l'impatto effettivo è stato minore rispetto alla valutazione di rischio effettuata negli anni scorsi. Solo a titolo di esempio di condizionamenti possibili, in svariate forme, pensiamo alle seguenti ipotesi: il condizionamento di elezioni attraverso la distruzione dell'immagine pubblica del candidato, o del partito o del movimento; la moltiplicazione dell'efficacia di discorsi d'odio, e quindi anche della radicalizzazione attraverso la

7) Il dato è abbastanza pacifico sia dal punto di vista empirico che nel quadro delle riflessioni sociologiche. Si veda, per chi è interessato all'approfondimento del tema, A. Plebani, *Jihadsmo globale. Strategie del terrore tra Oriente ed Occidente*, Giunti, 2016. In una prospettiva di studio particolare, prevalentemente psicoanalitica, si veda F. Benslama, *Un furioso desiderio di sacrificio. Il supermusulmano*, Raffaello Cortina Editore, traduzione italiana del 2017. Il giorno prima degli attentati coordinati di Parigi, Fethi Benslama aveva pubblicato su Le Monde l'articolo "*Pour le désespérés, l'islamisme radical est un produit excitant*" (12 novembre 2015). Altro noto psicoanalista, Luigi Zoja, ha trovato una felice espressione sintetica: "*La sensazione di esistere non è consegnata dalla vita, ma dalla morte*" (L. Zoja, *Nella mente di un terrorista. Conversazione con Omar Bellicini*, Einaudi, 2017, p. 73).
Sulla "*morte cercata*", sul significato e valore, sono numerosi i contributi di Olivier Roy (più recente: O. Roy, *Le djihad et la mort*, Editions du Seuil, 2016; traduzione italiana: O. Roy, *Generazione Isis. Chi sono i giovani che scelgono il califfato e perché combattono l'Occidente*, Feltrinelli, 2017). Per alcune riflessioni su ulteriori dati di esperienza vedi anche M. Romanelli, *Brevi note sulla prevenzione della radicalizzazione jihadista*, in *Sistema penale*, 20 marzo 2020.

rete, con l'ulteriore vantaggio di forme di anonimizzazione ancora più sicure.

Il contenuto audio-video falso o manipolato, realizzato attraverso sistemi di intelligenza artificiale, può avere efficacia devastante, sia per la qualità del falso che per la straordinaria capacità di disseminazione e per la velocità della stessa.

Nessuna contronarrazione, correzione, tentativo di eliminazione è in grado di sanare completamente l'effetto del falso.

Portando l'attenzione al mondo del terrorismo, emergono, nello specifico, due possibili riflessioni.

La propaganda online ha rappresentato uno dei più importanti fattori di successo del terrorismo c.d. islamico, così come la rete è il "luogo" d'eccellenza – non l'unico (pensiamo alle carceri) – per l'efficace funzionamento di meccanismi di radicalizzazione, e l'evoluzione tecnologica ha ovviamente contribuito in modo decisivo a questi successi.

Basti pensare che ai tempi delle Torri gemelle, e durante l'organizzazione delle stragi in Europa, il sistema per la chiamata all'azione, per il consolidamento di scelte radicali, per la adesione all'idea del martirio viaggiava ancora prevalentemente su carta o sulle "famose" audiocassette contenenti le immagini dei martiri, gli inni al martirio, i canti di battaglia, che venivano trasportate fisicamente e clandestinamente, con assunzione di gravi rischi, nei luoghi dell'ascolto in comune e della radicalizzazione.

È pacifico quindi che l'intelligenza artificiale in questo settore ha un presente ed un futuro.

Una (possibile) riflessione: la realtà, sapientemente montata ed illustrata, offre già di per se stessa grandi occasioni di contributo alla radicalizzazione, come l'esperienza delle investigazioni in materia ci ha dimostrato.

È sufficiente ricordare qui la "capacità" di radicalizzazione che hanno avuto da sempre le foto – pacificamente vere – delle varie forme di tortura che sono state utilizzate ad Abu Ghraib o le immagini degli "arancioni" di Guantanamo, che poi ritroveremo nelle tuniche fatte indossare agli ostaggi giustiziati dal nascente Stato Islamico.

Lo stesso effetto si è cercato di ottenere con le immagini terribili delle vittime dei bombardamenti, soprattutto bambini, accompagnate da frasi "classiche" di rivendicazione di attentati ("il vostro sangue è forse diverso dal nostro?", o frasi di contenuto analogo[8]).

8) Riproduco di seguito un passo della rivendicazione delle stragi dei treni di Madrid dell'11.3.2004, ma gli esempi offerti dall'esperienza sul campo delle indagini sono innumerevoli: "*... Sappiate che non avrete scampo e che Bush e la sua amministrazione vi porteranno solo distruzione. Noi vi uccideremo in ogni luogo ed in ogni tempo. Non ci sono differenze tra i civili ed i militari: le nostre vittime innocenti stanno morendo a migliaia in Afghanistan ed in Iraq. Il vostro sangue*

Questo non significa ovviamente che il deep-fake ha poco presente, o poco futuro, ma significa ancora una volta, e soltanto, fare i conti con i dati di realtà, e semmai ricordare con forza le regole di un sistema di contrasto al terrorismo che rispetti sempre i canoni di fondo del sistema penale costituzionale e del rispetto dei diritti.

Per chiudere, con formule di sintesi:

– massima attenzione all'innovazione tecnologica, sempre, ed ancora di più oggi, atteso che l'A.I. è dato di realtà, e di uso quasi comune;

– attenzione però sempre anche ai dati di conoscenza empirica dei fenomeni, alle ragioni delle scelte radicali, in una prospettiva di prevenzione/contrasto che individui le cause e che lavori su queste;

– ultimo: il rendere giustizia secondo le regole è il migliore antidoto al terrorismo ed alla visione radicale che lo sostiene; non è l'unico, e mai lo sarà, ma aiuta davvero. Questi principi valgono, e devono valere, anche con riferimento alle nuove sfide.

è più prezioso del nostro? Non avremo pietà con la vostra gente, vi uccideremo, porteremo la guerra nelle vostre case e voi non prenderete più sonno". Non molti dissimili i concetti espressi da Mohammad Sidique Khan, cittadino inglese, nella sua rivendicazione delle stragi di Londra del Luglio 2005: "*... Finchè voi non smetterete di bombardare, gassare, imprigionare e torturare il mio popolo, noi non termineremo questa lotta. Noi siamo in guerra ed io sono un soldato...*".

di Matteo Feraboli*

Questi ultimi anni hanno rappresentato un momento di profonda trasformazione, determinando un cambiamento radicale in molteplici elementi caratterizzanti la vita di cittadini, imprese e istituzioni. In tutti i settori della vita privata e pubblica, con velocità talvolta differenti e spesso senza una coerente sintonia, abbiamo assistito alla progressiva evoluzione di elementi sino a poco fa considerati esclusivamente "fisici", nella relativa trasposizione digitale:

– lo stesso concetto di "identità" si è via via trasformata in "digitale": dalle semplici utenze (*user-id e password)* necessarie per l'accesso ai molteplici servizi web, commerciali e di servizio, fino alla più recente introduzione di documenti digitali (CIE) e la conseguente progressiva spinta della PA verso un'identità digitale unica, necessaria per l'accesso ai servizi pubblici resi disponibili on-Line (SPID);

– abbiamo assistito ad una forte accelerazione nell'utilizzo di sistemi di pagamento digitali: dalle comuni transazioni elettroniche, legate alla forte evoluzione del commercio on-line, all'utilizzo di sistemi di pagamento alternativi a quelli "tradizionali", come i *wallet* di pagamento, sino alla più recente diffusione delle *crypto valute*;

– le stesse interazioni sociali si sono sempre più spostate dal mondo fisico al mondo digitale: i social network, ricreativi e professionali, il mondo dell'integrazione tra fisico e digitale, come il comparto delle tecnologie indossabili (*wearable device*), i luoghi ancora "fisici" ma senza più previsione di interazione umana, in cui si fa la spesa e si esce senza incontrare personale (*Amazon store*);

– il mondo del lavoro, con lo spostamento delle attività produttive dalle mura degli uffici al concetto di *Smart Working*, con il conseguente sviluppo dei sistemi di *tele presenza* e di "*collaboration*"; sino all'avvento del "*meta verso*", ambiente completamente digitale e popolato da *avatar* di cittadini, verso cui si sta orientando anche il mondo delle grandi Corporation, delle imprese e della PA (vedi il recente caso del Governo Sud Coreano).

Ciò che accomuna tutti questi grandi cambiamenti è la progressiva cancellazione del confine esistente tra il mondo del reale e il mondo del digitale.

(*) Cybersecurity e Fraud Management, Group Senior Director Cybersecurity & Anti-Fraud Services, Intesa Sanpaolo S.p.A.

Oltre alle informazioni relative alle transazioni effettuate nel digitale: pagamenti, abitudini di consumo, posizione geografica, gusti di visione, network di frequentazioni, professionali e private, le "*tracce* digitali" che il cittadino lascia a disposizione degli algoritmi, sono sempre più fluide e vengono arricchite attraverso i gesti quotidiani della nostra vita. Vengono tracciati i nostri dati ogniqualvolta interagiamo con la nostra auto, quando passiamo fisicamente in banca, ad una stazione di servizio, ma anche semplicemente al supermercato, o dando un esame all'università, o scorrendo un sito di prenotazioni online per il prossimo volo aereo o soggiorno.

Tutto ciò rappresenta una forte opportunità, rendendo più accessibili e trasparenti i servizi a disposizione del cittadino, migliorando per molti aspetti la qualità della vita, semplificando azioni che precedentemente avrebbero richiesto un maggiore dispendio di risorse e di tempo.

Alla stessa stregua, questa improvvisa accelerazione nel processo di digitalizzazione comporta anche molteplici rischi, legati ad elementi disruptive di contesto:

– aumento della superficie di attacco a favore di cyber criminali e frodatori: l'utilizzo di canali digitali da parte di tutte le classi della popolazione, a fronte di una non omogenea capacità tecnica da parte degli utilizzatori finali e di una generalizzata incuria in ambito "*cyber hygiene*", ha incrementato in modo significativo le opportunità di attacco da parte di hacker professionisti e di bande di "*frodatori* digitali";

– emergenza derivante dalla recente pandemia Sars-Cov-2, che ha incrementato le opportunità di frode, sfruttando da un lato la manifesta impossibilità di cittadini, imprese e istituzioni di agire tempestivamente attraverso i canali di interazione standard e, dall'altro, lo spostamento repentino di molteplici servizi esclusivamente su canali digitali;

– disponibilità di strumenti digitali "*offensivi*": la così detta "*commoditizzazione*" o "*industrializzazione*" degli strumenti di hacking ha determinato un netto ampliamento della platea dei possibili attaccanti, rendendo disponibili anche a malviventi poco avvezzi alla tecnologia e allo sviluppo software strumenti digitali offensivi "*pronti per l'uso*": sistemi per la gestione di campagne di phishing, data base di credenziali sottratte ai cittadini per effetto di data breach a istituzioni e imprese private, *malware* e *trojan bancari* personalizzabili in relazione alle necessità dei frodatori, ecc;

– debolezze di sistema. La velocità di digitalizzazione e, in alcuni casi, precise scelte industriali, espongono i cittadini a una serie di vulnerabilità di sistema che incidono negativamente sulla capacità di difesa delle vittime di frodi on-line. Esempi lampanti sono il caso del "*sms alias spoofing*", ovvero

la possibilità di alterare in modo molto semplice il mittente di un sms malevolo, recapitandolo in modo che sembri inviato da un'istituzione legittima (una Banca, un'amministrazione pubblica, un negozio online, ecc.), *il* "*call-id spoofing*", ovvero la possibilità di telefonare modificando il proprio numero chiamante e impersonando quindi un servizio legittimo (un call center, un centro di assistenza, ecc.).

In questo contesto, gli strumenti a disposizione degli attaccanti risultano via via sempre più semplici da identificare e utilizzare. Senza dover ricorrere a risorse di più difficile reperibilità (i così detti "*dark and deep web*"), una semplicissima ricerca su un motore di ricerca pubblico consente di identificare risorse offensive pronte all'uso e a prezzi modici.

1. Evoluzione della strategia di sicurezza

In risposta a questo quadro di complessità, la Banca ha identificato alcune macro aree di rischio verso cui far convergere risorse economiche e professionali, con la finalità di incrementare i propri sistemi di difesa e di incrementare la consapevolezza digitale dei cittadini:

– la protezione dei propri clienti da frodi;

– la difesa delle proprie infrastrutture, in quanto di interesse nazionale per un soggetto di impatto sistemico;

– il continuo adattamento ai nuovi e sempre più stringenti requisiti normativi e legislativi, anch'essi derivanti dal rapido cambiamento di contesto.

Il mutato contesto ha richiesto di ripensare in modo critico le strategie di sicurezza, evolvendo i paradigmi esistenti e basati su un concetto di "*sicurezza di* confine", ovvero volti a proteggere l'organizzazione guardando ad un ideale perimetro fisico, e "*siloed*", cioè mantenendo una significativa separazione tra le componenti organizzative Cyber, Anti-Frode, Network e Threat Intelligence, ad un approccio pervasivo, orizzontale, sicuro "*by design*" e sempre più "*data driven*" ovvero, sfruttando in senso offensivo e difensivo l'enorme quantità di dati a nostra disposizione.

Il concetto di "*Security by Design*" introduce un processo end to end, un modello volto a gestire e verificare tutti gli aspetti di sicurezza nell'ambito di ogni fase del ciclo di vita di un'iniziativa aziendale, sia essa di business o meramente tecnologica. Il principio guida deriva da una continua analisi e valutazione del rischio, che determina la definizione dei requisiti di sicurezza, dinamici e variabili, in relazione alla concreta esposizione al rischio e al mutare delle minacce.

Questo approccio evoluto ha comportato il rafforzamento dei processi di Cyber Threat Intelligence e delle nostre capacità complessive di analisi, attraverso l'integrazione di fonti eterogenee derivanti da fonti informative eterogenee: interne, prodotte da Terze Parti e disponibili attraverso fonti aperte (OSINT).

Da un punto di vista organizzativo, si è rafforzata in modo significativo la convergenza tra i team Cyber e Anti-Frode, creando processi trasversali e momenti di scambio informativo strutturati, e incrementando progressivamente la rete del Global CSIRT (*Computer Security Incident Response Team*) non solo alle Legal Entity straniere afferenti al Gruppo ISP, ma anche a un selezionato gruppo di significative Terze Parti commerciali, in un'ottica di "*democratizzazione dell'intelligence*".

2. Attuali applicazioni AI/ML in ambito Cyber Security e Anti-Frode

In ambito Cyber Security, la disponibilità di soluzioni che fanno uso di tecniche di Intelligenza Artificiale e Machine Learning è via via sempre più pervasiva. Più dell'80% delle soluzioni Cyber Security commerciali attualmente in uso presso il Gruppo ISP ricade in questo cluster.

A titolo di esempio, le soluzioni EDR (*Endpoint Detection and Response)* agiscono in modalità variabile, sfruttando telemetrie elaborate nel Cloud ed applicando sofisticati algoritmi di Machine Learning, volti a identificare proattivamente comportamenti anomali, sintomo di potenziale compromissione dell'endpoint; i sistemi anti-spam, al pari, possono contare sull'elaborazione di un'ingente mole di dati, afferenti a molteplici organizzazioni commerciali e analizzate da algoritmi AI per raffinare continuamente la capacità di detection di mail malevole (quasi il 70% delle email in circolazione). Sistemi AI e ML entrano in gioco anche nell'analisi continua del traffico di rete, verificando il comportamento dei protocolli di comunicazione alla ricerca di anomalie che altrimenti non potrebbero essere identificate dagli analisti di Cyber Security.

Anche il sistema SIEM (Security Information and Event Management) in uso al Global Security Operation Center (GSOC), ovvero la piattaforma verso cui convergono tutte le telemetrie e gli eventi di sicurezza generati dai sistemi di sicurezza e applicativi di tutto il Gruppo ISP, fa uso di un sistema basato su AI. Tale sistema agisce a supporto degli analisti di primo e di secondo livello, con la finalità di identificare in modo autonomo eventi di bassa frequenza, potenzialmente sottovalutati dagli analisti, eventi che potrebbero

rappresentare indici di compromissione particolarmente sofisticati.

Nell'ambito della prevenzione delle frodi informatiche e delle truffe finanziarie, la Banca ha adottato molteplici sistemi predittivi basati su motori AI e ML. L'obiettivo di questi oggetti è quello di rendere sempre più trasparente all'utente finale il sistema di sicurezza, supportandolo in modo efficace nell'identificazione proattiva delle minacce a cui è esposto.

Un esempio molto efficace di queste tecnologie è rappresentato dal sistema BCM (*Behavioural Customer Monitoring*). Attraverso questo algoritmo, per ciascun cliente vengono costruiti indicatori specifici e personalizzati. Si analizzano con altissima precisone le abitudini finanziarie di ciascun cliente, basandosi sull'operatività, i dati tipici di posizione geografica, i device in uso e un vastissimo numero di altre informazioni raccolte nel pieno rispetto dei diritti di privacy dell'interessato. Questo sistema ha consentito di ridurre drasticamente molteplici fenomenologie frodatorie che avevano visto nel periodo più acuto della pandemia Sars-Cov-2 picchi vertiginosi.

Tali algoritmi vengono continuamente arricchiti con nuove classi di informazioni, migliorando l'efficacia complessiva del modello.

Il percorso evolutivo prevede la futura introduzione di informazioni derivanti dal riconoscimento biometrico del cliente, così da incrementare ulteriormente l'efficacia del sistema e rendere trasparente all'utente finale i processi autorizzativi e di continua autenticazione ai servizi bancari.

L'evoluzione delle minacce e la sofisticazione degli attacchi perpetrati da hacker e frodatori sollecitano ad un continuo processo di revisione e affinamento di tutti i presidi di difesa, spostando il focus da un approccio reattivo ad un orientamento sempre più proattivo. In questo percorso, i sistemi AI e ML via via implementati e affinati giocano un ruolo fondamentale.

L'evoluzione descritta passa anche attraverso la revisione degli attuali modelli organizzativi e dei nostri processi investigativi.

In questo ambito si colloca l'evoluzione del GSOC verso un approccio "*Fusion Center*": una profonda trasformazione dei paradigmi di monitoraggio e correlazione eventi, che comporta una totale convergenza tra il mondo Cyber e quello del contrasto alle frodi. Questo processo prevede la progressiva raccolta di qualsiasi tipologia di telemetria generata in ambito Cyber Security Defence, Threat Intelligence, Applicativa, Anti-Frode in un unico *Data Lake*, a disposizione di sofisticati sistemi di ML, finalizzati all'identificazione predittiva di fenomeni offensivi anche a bassa frequenza, potenzialmente impossibili da identificare da parte di sistemi di monitoraggio tradizionali.

L'evoluzione dei nostri processi investigativi ha consentito l'ideazione e lo sviluppo di una nuova figura professionale, denominata "*Etichal Fraud-*

ster". Il termine, mutuato dal mondo della Cyber Security (Ethical Hacker), prevede lo sviluppo di competenze, attività e strumenti investigativi atti a identificare proattivamente fenomeni frodatori emergenti, ovvero prima che possano causare danni su larga scala. Le prime esperienze sviluppate in questo contesto hanno consentito di identificare e rendere inoffensivi alcuni pattern frodatori, con un beneficio diretto per l'intero settore bancario, nazionale ed internazionale.

Le problematiche concorrenziali e consumeristiche in ambito digitale

di Jacques Moscianese*

1. Le norme antitrust nel mondo digitale: la c.d. *algorithmic collusion*

Fra gli strumenti ormai tipici del mondo digitale vi sono gli algoritmi. In particolare, *monitoring*, *parallel*, *signalling* e *self-learning algorithm* (OECD, 2017) sono ormai ampiamente adottati in molti settori dell'economia, con conseguenze pro-competitive e garantendo maggiore efficienza alle imprese.

Tuttavia, l'utilizzo di tali algoritmi può essere fonte di problematiche concorrenziali. Infatti, è stato evidenziato in dottrina (Ezrachi, Stuke, 2016) che i citati algoritmi potrebbero rappresentare mezzi adatti a permettere alle imprese di colludere fra loro sui parametri competitivi (su tutti, il prezzo). Questa collusione può essere tanto tacita, ovvero raggiunta senza la necessità di contatti o scambi di informazioni fra concorrenti, oppure esplicita, ossia perseguita per il tramite di una vera e propria concertazione fra competitor.

Nel contesto del diritto antitrust europeo ed italiano, soltanto la seconda tipologia di collusione (quella esplicita) rientra nella nozione di pratica concordata e – di conseguenza – può essere sanzionata dall'ordinamento, qualora abbia oggetto o effetto anticoncorrenziale (art. 101 TFUE e art. 2 legge 287/1990). Ai sensi della giurisprudenza della Corte di giustizia UE, una pratica concordata, infatti, "implica una forma di coordinamento fra imprese che, senza essere spinta fino all'attuazione di un vero e proprio accordo, sostituisce consapevolmente una collaborazione pratica fra le stesse ai rischi della concorrenza" (*T-Mobile*, 2009). Identica definizione è contenuta anche nella giurisprudenza del Consiglio di Stato (sentenza n. 5885, 2020).

Secondo le più recenti prese di posizione della Commissione UE, l'uso di algoritmi può facilitare la stabilità di un coordinamento anticoncorrenziale fra imprese. In altri termini, "gli algoritmi possono consentire ai concorrenti di aumentare la trasparenza del mercato, individuare scostamenti sui prezzi in tempo reale e rendere più efficaci i meccanismi sanzionatori". Ciò in particolare, in presenza di "alcune condizioni strutturali di mercato, quali un'elevata frequenza di interazioni, un potere limitato degli acquirenti e la presenza di

(*) Executive Director Institutional Affairs, Intesa Sanpaolo S.p.A.

prodotti/servizi omogenei" (Commissione UE, 2022). Chiaramente, in questo caso la Commissione UE non solo si riferisce agli algoritmi come mezzo per rendere più stabile una concertazione già in atto con altri mezzi, ma inoltre inquadra la loro analisi antitrust nel contesto delle violazioni per effetto, dato l'accento che pone sulle condizioni strutturali del mercato, come presupposto per rendere possibile la collusione (anche) algoritmica.

Al contrario, la Commissione UE ritiene che altri tipi di concertazione per il tramite di algoritmi siano da qualificarsi come violazioni per oggetto, ossia infrazioni del diritto antitrust che per loro natura sono tanto gravi da rendere del tutto superflua un'analisi degli effetti (attuali o potenziali) della condotta (*Beef Industry*, 2008). In particolare, la c.d. collusione mediante codice, secondo la Commissione UE, corrisponderebbe ad un'applicazione "deliberata da parte di concorrenti di algoritmi comuni di coordinamento comportamentale", costituendo quindi un cartello, ossia una restrizione della concorrenza per oggetto, "indipendentemente dalle condizioni di mercato e dalle informazioni scambiate" (Commissione UE, 2022). In questo caso, a differenza di quanto detto sopra, sembra che sia la stessa adozione dell'algoritmo comune fra concorrenti a costituire il centro della pratica concordata. L'algoritmo non facilita una collusione già in essere, ma è esso stesso il mezzo principale della concertazione anticoncorrenziale.

Infine, sempre la Commissione UE suggerisce che gli algoritmi possano essere utilizzati per una c.d. collusione indiretta (*hub-and-spoke collusion*). Invero, l'aggregazione di informazioni sensibili in uno strumento di fissazione dei prezzi, offerto da un comune consulente informatico (c.d. algoritmo condiviso) a cui vari concorrenti hanno accesso, potrebbe costituire una collusione orizzontale (Commissione UE, 2022), di cui siano responsabili tanto i concorrenti che vi partecipano, quanto il comune consulente, nonostante quest'ultimo non operi nel mercato in cui avviene la collusione (*AC-Treuhand*/*Commissione*, 2015).

Tuttavia, al netto delle prese di posizione delle autorità, è bene ribadire quanto detto sopra con riferimento alla giurisprudenza della Corte di giustizia UE (e del Consiglio di Stato), ovvero che la nozione di pratica concordata presuppone che le imprese che vi prendono parte siano consapevoli di partecipare ad una forma di concertazione. Insomma, affinché un'impresa sia ritenuta responsabile di una concertazione anticoncorrenziale è necessario che tale impresa sia a conoscenza (o non possa non essere a conoscenza) di farne parte (*Eturas*, 2016).

Pertanto, qualora imprese fra loro concorrenti monitorino le reciproche attività sul mercato affidandosi ad algoritmi, senza però ingaggiare una vera

e propria concertazione (fatta quindi di contatti e scambi di informazioni fra loro), tale attività non può essere ricondotta ad una pratica concordata. Al contrario, si tratta di una condotta (unilaterale) del tutto legittima di raccolta di informazioni pubblicamente disponibili sulle strategie dei propri concorrenti che può condurre a un parallelismo di comportamento fra imprese sul mercato.

Per quanto tale monitoraggio possa portare a condizioni sul mercato analoghe a quelle che potrebbero essere conseguenza di una concertazione, proprio l'assenza di quest'ultima impedisce all'ordinamento di sanzionare il mero comportamento parallelo sul mercato. Come stabilito dalla Corte di giustizia UE, infatti, la comunicazione di informazioni sui prezzi al mercato da parte di un'impresa e il monitoraggio di tali informazioni da parte dei suoi concorrenti (con conseguente parallelismo di comportamento) non sono azioni capaci di ridurre le incertezze delle imprese coinvolte circa il futuro atteggiamento dei concorrenti. Infatti, ciascuna impresa – all'atto di comunicare i propri prezzi al mercato – non ha alcuna certezza circa il comportamento che sarà adottato dalle altre. In altri termini, quando la spiegazione del parallelismo di comportamenti basata sulla concertazione non è l'unica plausibile, il parallelismo non può costituire, preso singolarmente, la prova di una pratica concordata (*Ahlström Osakeyhtiö/Commissione*, 1993).

Il criterio della consapevolezza proprio della nozione di pratica concordata è, perciò, il principale ostacolo (se così si può dire) per qualificare il mero uso di un algoritmo da parte di imprese operanti sul mercato fra loro in concorrenza come l'attuazione di una pratica concordata. Qualora tale consapevolezza sia presente, come nel caso della c.d. collusione mediante codice a cui si riferisce la Commissione UE, la riconduzione dell'utilizzo dell'algoritmo alla fattispecie di pratica concordata sarà agevole.

2. Le norme a tutela del consumatore nel mondo digitale: il caso *Facebook* (2018)

Per ciò che attiene ai profili consumeristici dell'economia digitale, è di sicuro interesse il caso Facebook trattato dall'Autorità Garante della Concorrenza e del Mercato (AGCM) nel 2018 e oggetto, successivamente, di pronunce della giustizia amministrativa.

Secondo AGCM, Facebook aveva posto in essere due c.d. pratiche commerciali scorrette, ai sensi del Codice del consumo. In base alla prima, consistente in una pratica ingannevole, AGCM riteneva che Facebook non

informasse l'utente senza indugio del fatto che i suoi dati sarebbero stati raccolti e utilizzati per finalità informative e/o commerciali. Invero, in fase di attivazione dell'account, l'utente veniva reso edotto solo della gratuità del servizio (ossia che registrarsi a Facebook non comporta costi in termini pecuniari), venendo così indotto ad assumere una decisione di natura commerciale che, altrimenti, non avrebbe preso.

La seconda pratica contestata a Facebook era, invece, una pratica c.d. aggressiva. Secondo AGCM, infatti, l'utente avrebbe ceduto i propri dati tramite un sistema di preselezione operato da Facebook; così facendo, i consumatori, in cambio dell'utilizzo del sito, sarebbero stati costretti a consentire alla piattaforma social e a terzi la raccolta e l'utilizzo, per finalità informative e/o commerciali, dei dati che li riguardavano.

Di conseguenza, in data 29 novembre 2018, AGCM sanzionava Facebook per Euro 5 milioni per la pratica ingannevole e per altri Euro 5 milioni per pratica aggressiva. Inoltre, AGCM prevedeva l'adozione di misure atte a far cessare le pratiche ingannevole e aggressiva, così come l'obbligo di Facebook di pubblicare una dichiarazione rettificativa in cui il social network comunicava pubblicamente l'esito dell'indagine dell'Autorità.

In sede di ricorso al TAR Lazio, Facebook sosteneva che il Codice del consumo non poteva trovare applicazione all'apertura di un account presso il suo social network, in quanto il trattamento dei dati da parte di Facebook sarebbe stato inquadrabile esclusivamente come fattispecie regolata dalle norme relative alla tutela della privacy e non da quelle a tutela del consumatore. In altri termini, secondo Facebook l'apertura di un account non era qualificabile come rapporto di consumo.

Tuttavia, tanto il TAR Lazio (sentenza n. 260, 2020), prima, quanto il Consiglio di Stato (sentenza n. 2631, 2021), poi, hanno confermato l'applicabilità delle norme a tutela del consumatore al rapporto instaurato fra Facebook e l'utente quando quest'ultimo apre un account, alla luce del fatto che – usando le parole del Consiglio di Stato – un diritto personalissimo, come quello all'uso dei propri dati, è nei fatti "sfruttato" a fini commerciali, indipendentemente dalla volontà dell'interessato utente-consumatore.

A seguito del giudizio del Consiglio di Stato, la pratica ingannevole è stata confermata, in quanto "omette informazioni rilevanti di cui il consumatore necessita al fine di assumere una decisione consapevole di natura commerciale quale è quella di registrarsi nella Piattaforma Facebook". Al contrario, la pratica aggressiva è stata annullata, perché «la "pre-attivazione" della piattaforma Facebook (vale a dire la "preselezione" delle opzioni a disposizioni) […] non comporta alcuna trasmissione di dati in modo diretto ed

immediato dalla piattaforma di FB a quella di soggetti terzi».

Ad ogni buon conto, le maglie strette della rete rappresentata dal Codice del consumo sono state in grado di cogliere i comportamenti del principale social network e di sanzionarlo per violazioni delle norme consumeristiche. Ciò dimostra, se ve ne fosse il bisogno, la maggiore flessibilità delle norme a tutela del consumatore rispetto a quelle antitrust. Non è un caso, quindi, che ad oggi siano stati diversi – in Italia e nel resto degli Stati membri UE – gli interventi sulle grandi piattaforme che dominano il mondo digitale ai sensi delle norme sulle pratiche commerciali scorrette, mentre minori (o quantomeno più difficoltosi) siano stati i casi aperti in base alle norme a tutela della concorrenza.

Bibliografia

Commissione UE, *Proposta di Comunicazione contenente nuove "Linee direttrici sull'applicabilità dell'articolo 101 del trattato sul funzionamento dell'Unione europea agli accordi di cooperazione orizzontale"*, 2022

Consiglio di Stato, sentenza sez. VI, 06.10.2020, n. 5885

Consiglio di Stato, sentenza sez. VI, 29.03.2021, n. 2631

Ezrachi A. - Stucke M.E. (2016), *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy*, Harvard University Press, United States

OECD (2017), *Algorithms and Collusion: Competition Policy in the Digital Age*, in *www.oecd.org/competition/algorithms-collusion-competition-policy-in-the-digital-age.htm*

PS11112, *Facebook - Condivisione dati con terzi*, Provvedimento n. 27432

Sentenza della Corte di giustizia UE, 20 novembre 2008, C-209/07, *Beef Industry*, ECLI:EU:C:2008:643

Sentenza della Corte di giustizia UE, 21 gennaio 2016, *Eturas*, C-74/14, ECLI:EU:C:2016:42

Sentenza della Corte di giustizia UE, 22 ottobre 2015, *AC-Treuhand/Commissione*, C-194/14 P, ECLI:EU:C:2015:717

Sentenza della Corte di giustizia UE, 31 marzo 1993, *Ahlström Osakeyhtiö/Commissione*, cause riunite C-89/85, C-104/85, C-114/85, C-116/85, C-117/85 e C-125/85 a C-129/85, ECLI:EU:C:1993:120

Sentenza della Corte di giustizia UE, 4 giugno 2009, C-8/08, *T-Mobile*, ECLI:EU:C:2009:343

TAR Lazio, sentenza sez. I, 10.01.2020, n. 260

di Carlo Nardello,
con il contributo di Giuseppe Roberto Marseglia e Lorenzo Iannarilli*

1. La digital literacy come arma di inclusione e sicurezza

Ogni anno, intorno a novembre, la Commissione Europea pubblica il rapporto DESI (The Digital Economy and Society Index), un rapporto utile a riassumere gli indicatori sulle prestazioni digitali dell'Europa e a tracciare i progressi dei Paesi dell'Unione. Il rapporto del 2021 mostra un'Europa che sui temi digitali viaggia a due velocità: da una parte gli stati del nord Europa, che mostrano performance ottime rispetto a tutte le dimensioni di misura, dall'altra gli stati dell'Europa dell'est, a cui si sommano Portogallo ed Italia, che invece mostrano performance pessime in tutte (o quasi) le dimensioni di misura.

Nell'ultimo anno l'Italia ha mostrato un miglioramento importante rispetto all'anno precedente, ma rispetto alla dimensione del *human capital*, si classifica ancora tra gli ultimi posti in Europa e addirittura ultima per quanto riguarda le "*advanced skills*". Il risultato dell'analisi suggerisce dunque che le imprese italiane abbiano urgente bisogno di promuovere azioni di trasformazione digitale e programmi di innovazione strutturati e che la diffusione di competenze digitali sia di base (*digital literacy*) che avanzate debba essere una priorità strategica.

Se da un lato, infatti, i cittadini italiani stentano a recuperare le conoscenze di base per cogliere le nuove opportunità e schivare le nuove insidie proposte dalla *digital era*, l'economia globale invece accelera e propone azioni strutturali che puntano a rendere le nostre città vere e proprie città connesse ed hub multiservizio di respiro internazionale (*smart cities*) e che spingono le imprese a ripensarsi e compiere vere e proprie *business model revolutions* in cui i cosiddetti *smart products* – i prodotti, cioè, che hanno degli elementi *smart* al loro interno – sono ceduti al consumatore non tramite vendita ma tramite *servitizzazione*. Il consumatore si lega quindi non più con un acquisto, ma con un abbonamento alle società comprando il tempo di utilizzo di un bene e non il bene stesso (e.g. Car2Go, EniJoy, Netflix, ecc).

(*) Carlo Nardello, Docente (a.c.), Università "Sapienza" e Lumsa; Giuseppe Roberto Marseglia, CEO @ Daat Consulting; Lorenzo Iannarilli, Cultore della materia, Università Lumsa.

2. Il metaverso: un mondo di mondi

Oltre alla accelerazione *pull* – legata quindi alle necessità proposte dal mercato che evolvono e richiedono servizi sempre più automatizzati, sempre più rapidi e con la creazione di valore sempre più vicino al consumatore – è in corso una seconda spinta, una accelerazione *push,* legata alla rapida evoluzione delle tecnologie. La quarta rivoluzione industriale o Industry 4.0, che vede protagonisti i dati e la connettività digitale e che è ancora in corso, infatti, rispetto al passato propone sfide originali cui dobbiamo rispondere prontamente e con i giusti strumenti. In particolare, differentemente dalle precedenti rivoluzioni in cui la tecnologia evolveva lentamente durante le fasi di cambiamento, oggi si parla di una fase comunemente nota come *age of accelerating change* o fase di *exponential growth of technology* in cui in un tempo che varia dai tre ai sette anni circa i paradigmi tecnologici cambiano quasi completamente essendo quindi delle piccole rivoluzioni tecnologiche all'interno di una più grande rivoluzione industriale.

A titolo esemplificativo, negli ultimi anni le tecnologie che hanno raggiunto piena maturazione e che possono essere oramai considerate un driver per la generazione di valore da parte delle imprese sono *cloud computing, artificial intelligence, IIoT - industrial internet of things, connettività 5G, blockchain* e, ultima in ordine di tempo, il *metaverso.*

A dire il vero, il concetto di metaverso è tutt'altro che nuovo: il termine è stato coniato dall'autore Neal Stephenson nel romanzo fantascientifico *Snow Crash* uscito nel 1992 in cui gli esseri umani sono descritti come avatar programmabili che interagiscono tra di loro e con agenti software all'interno di uno spazio virtuale tridimensionale.

La definizione precisa di metaverso è ad oggi molto dibattuta. Alla fine del 2021, quasi trent'anni dopo l'uscita del romanzo di Neal Stephenson, Mark Zuckerberg, fondatore di Facebook, ha annunciato che avrebbe cambiato il nome dell'azienda da Facebook a Meta e che avrebbe costruito un mondo virtuale – Horizon – che fosse un *insieme di spazi virtuali* che consentono di creare, esplorare ed *interagire con persone* che però *non sono necessariamente nello stesso spazio fisico*.

La definizione che il fondatore di Facebook ha dato del metaverso è certamente semplice e molto comprensibile, ma alle volte criticata proprio per la – forse – eccessiva semplificazione e le definizioni tecniche date successivamente vengono complicate facendo spesso menzione di economia, scarsità di risorse, blockchain, scambio di beni, ecc.

Dare una definizione precisa di metaverso oggi, d'altra parte, è forse

prematuro e anche poco utile. È invece importante cercare di tracciare dei confini funzionali rispetto alle opportunità che il metaverso propone. In questo senso, il framework oggi comunemente accettato è quello proposto da un gruppo di accademici nel whitepaper "*A metaverse roadmap*" in cui vengono identificate quattro macro-categorie in cui suddividere le applicazioni legate al metaverso.

La prima, i *mirror worlds,* fa riferimento ai modelli riflessi del mondo fisico, a tentativi, cioè, di riprodurre *in silico* la realtà fisica nella maniera più realistica possibile. Gli esempi tipici dei *mirror worlds* sono i *digital twins,* o gemelli digitali, strumenti utili a simulare – ad esempio – la tenuta di un ponte sottoposto a forti sollecitazioni con una simulazione a computer e senza la necessità di sollecitare un ponte reale con il rischio che crolli.

La seconda, i *virtual worlds*, fa riferimento a mondi virtuali che non necessariamente trovano corrispondenza nel mondo fisico rispetto alle azioni possibili che è consentito fare. Un esempio tipico – anche se un po' datato – è *Second Life* che consente ai giocatori di costruirsi una vita in un mondo virtuale in cui è – tra le altre cose – possibile volare e teletrasportarsi.

La terza, l'*augmented reality*, fa riferimento a tutte le applicazioni che consentono di inserire elementi virtuali all'interno del mondo fisico. Mentre la fruizione di applicazioni di *augmented reality* è stata lungamente vincolata all'utilizzo dei visori, oggi è possibile sviluppare applicazioni anche utilizzando esclusivamente il cellullare degli utenti. L'esempio più tipico in questo senso è *PokemonGo*.

La quarta ed ultima, il *life logging*, fa riferimento a tutte le applicazioni che consentono di creare una traccia digitale di eventi fisici. L'esempio più tipico è l'*Apple Watch*.

Alcuni degli esempi sopracitati non sono certamente riferimenti ad applicativi e prodotti recenti. Ci sono, però, almeno due motivi per cui proprio oggi il metaverso è diventato una tematica da essere presa in seria considerazione dai consumatori e dalle aziende.

Il primo è dovuto ad un trend legato alle modalità di fruizione di servizi e prodotti per cui sempre più spesso le *customer journeys* degli utenti vengono descritte dalle aziende come *O2O* (i.e. *online-to-offline* e *offline-to-online*). In un'esperienza *multi-touchpoint*, quindi, non ci saranno solamente *touchpoints* digitali né solamente *touchpoints* fisici e il metaverso cerca di costruire dei punti nella *journey* che abbiano tutti i vantaggi del digitale e anche tutti i vantaggi del fisico. Un esempio tipico di un'esperienza *O2O* è rappresentato dal marchio di abbigliamento statunitense Bonobos, marchio che nasce esclusivamente online e che solo recentemente ha aperto dei "*guide shops*", dei

negozi fisici, cioè, dove è possibile recarsi per provare i vestiti che vengono acquistati in loco ma spediti solo in un secondo momento a casa. In questa maniera è possibile ottimizzare il magazzino (lato *merchant*) ed è possibile fare brevi sessioni di shopping in pausa pranzo senza la necessità di portarsi delle borse dietro tutto il giorno (lato cliente).

Il secondo motivo è dovuto alla rapida e contestuale maturazione di tecnologie abilitanti lo sviluppo di esperienze nel metaverso. Tra queste, le più rilevanti, la *blockchain*, il *cloud-computing*, l'intelligenza artificiale.

3. Luddismo digitale, rifiuto della tecnologia come sfida

Secondo i dati della World Bank solo il 70% degli italiani ha utilizzato servizi internet per almeno una volta nella vita e questo dato, che evidenzia ancora una volta l'*under-utilization* dei servizi di connettività e la scarsa digitalizzazione della popolazione, impatta in maniera più rilevante nelle fasce d'età avanzate rispetto alle generazioni più giovani. Recuperare il *digital divide* generazionale è una azione tanto necessaria quanto difficile. I continui aggiornamenti dei paradigmi tecnologici cui siamo soggetti, infatti, stimolano movimenti contrari al progresso e all'innovazione molto energici oggi noti come *digital luddism* e, nel migliore dei casi, una leggera ma decisa forma di rifiuto.

Contemporaneamente, però, l'età media degli utenti di *Roblox*, tra i più noti metaversi che oggi sono disponibili sul mercato, è di 13 anni circa. Chi può controllare che l'attività svolta su questi nuovi sistemi da parte dei giovanissimi non sia pericolosa se i loro genitori non hanno nemmeno gli strumenti per capirlo? Il metaverso non è, infatti, una tecnologia che arriverà nel prossimo futuro; fa parte già oggi nelle abitudini di interazione delle giovani generazioni che considerano normale l'acquisto e l'utilizzo di soldi virtuali per vestire e personalizzare il proprio avatar.

Bibliografia

Adeli E. et al., *Representation learning with statistical independence to mitigate bias*, Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision, 2021

Awad E. et al., *The moral machine experiment*, Nature 563.7729 (2018): 59-64.

Bughin J. - Catlin T. - Hirt M. - Willmott P., *Why digital strategies fail*, McKinsey Quarterly (2018)

Caputo B. et al., *Programma Strategico Intelligenza Artificiale 2022-2024*, Governo italiano (2021)

Cassard A. - Hamel J., *Exponential Growth of Technology and the Impact on Economic Jobs and Teachings: Change by Assimilation*, in *Journal of Applied Business & Economics*, 20.2 (2018)

Dai X., *Toward a reputation state: the social credit system project of China*, available at SSRN 3193577 (2018)

Dent E.B. - Goldberg S.G., *Challenging "resistance to change"*, in *The Journal of applied behavioral science*, 35.1 (1999): 25-41

European Commission, Directorate-General for Communications Networks, Content and Technology, *Ethics guidelines for trustworthy AI*, Publications Office, 2019, in *https://data.europa.eu/doi/10.2759/177365*

European Commission, *Proposal for a regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts*, 29.4.2021, European Union (2021), in *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021PC0206&from=EN*

European Commission, *The Digital Economy and Society Index*, European Union (2021)

European Commission, *White paper on Artificial Intelligence - A European approach to excellence and trust*, 19.2.2020, COM (2020), in *https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf*

European Parliament, *Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act)*, 2020

European Parliament, *Directive 2001/95/EC of the European Parliament and of the council on general product safety*, 3.12.2001, in *Official Journal of the European Union* (2001), su *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001L0095&from=EN*

European Parliament, *Directive 2006/42/EC of the European Parliament and of the council on machinery and amending Directive 95/16/EC (re-cast)*, 17.5.2016, in *Official Journal of the European Union* (2006), su *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006L0042&from=EN*

European Parliament, *Directive 2014/53/EU of the European Parliament and of the council on the harmonisation of the laws of the Member States*

relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC, 16.4.2014, in *Official Journal of the European Union* (2014), su *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0053&from=IT*

European Parliament, *Regulation 2016/679 of the European Parliament and of the council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, 27.4.2016, in *Official Journal of the European Union* (2016), su *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN*

Jones S.E., *Against technology: From the Luddites to neo-Luddism*, Routledge, 2013

Kaczynski T.J., *Industrial society and its future*, 1995

Marseglia G.R. - Dal Mas F. - Massaro M. - Bagnoli C., *L'Artificial Intelligence Act: risvolti pratici dell'etica dell'Intelligenza Arificiale*, in Vjollca Kopsaj (ed.), "Problemi di filosofia pratica 2021", Pavia, Printservice editore (2021), ISBN: 9788898765980

Marseglia G.R., *AI Act: impatti e proposte*, in rivista semestrale on-line *www.i-lex.it*, 2021

Popkova E.G. - Ragulina Y.V. - Bogoviz A.V., *Fundamental differences of transition to industry 4.0 from previous industrial revolutions*, Industry 4.0: Industrial Revolution of the 21st Century. Springer, Cham, 2019. 21-29

Senate of the United States, *Clarifying Lawful Overseas Use of Data (Cloud) Act*, 2018

Smart J. et al., *Metaverse Roadmap: A Cross-Industry Public Foresight Project*"

Taal A., *The GDPR Challenge: Privacy, Technology, and Compliance in an Age of Accelerating Change*, CRC Press, 2021

Thomson J.J., *Killing, letting die, and the trolley prob-lem*, The Monist 59.2 (1976): 204-217

Van Dijk J., *The digital divide*, John Wiley & Sons, 2020

Von der Leyen U., *Un'Unione più ambiziosa. Il mio pro-gramma per l'Europa*, European Union, 2019

White House (2022), *A declaration for the future of the internet*, in *https://www.whitehouse.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet_Launch-Event-Signing-Version_FINAL.pdf*

Zetzsche D.A. et al., *Regulating a revolution: from regulatory sandboxes to smart regulation*, Fordham J. Corp. & Fin. L. 23 (2017): 31

Criminalità informatica e intelligenza artificiale. Intelligenza Artificiale & Market Abuse

di Gaetano Ruta, Alberto Tavani e Stefano Scaroina*

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[1].

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.

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, nella sua sintetica esposizione, si articola su una ricognizione dei nodi applicativi sinora emersi e sulle risposte che il diritto può provare a dare, soprattutto nella prospettiva penalistica (che non è l'unica e che probabilmente, più di altre, si espone a difficoltà ed insidie).

(*) Gaetano Ruta, Procuratore Europeo Delegato, sede di Milano; Alberto Tavani, Direttore Innovazione, Trasformazione e Operations presso Cassa Depositi e Prestiti; Stefano Scaroina, Responsabile Compliance e Antiriciclaggio presso Cassa Depositi e Prestiti.

1) Il presente scritto costituisce la sintesi di un articolo pubblicato, sempre per conto della Fondazione Occorsio, sulla rivista online *Sistema penale*. Ad esso deve quindi farsi rinvio per eventuali approfondimenti (*https://www.sistemapenale.it/it/documenti/intelligenza-artificiale-e-giurisdizione-penale-fondazione-occorsio-atti-workshop*).

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*)»[2]. 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 divenire vittime delle condotte stesse[3].

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. 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 obbligazio-

2) Cfr. C. Schena - A. Tanda - C. Arlotta - G. Potenza, *Lo sviluppo del FinTech*, in *Quaderni FinTech*, Consob, 1/2018, su *https://www.consob.it/documents/46180/46181/FinTech_1.pdf/35712ee6-1ae5-4fbc-b4ca-e45b7bf80963#page=15*.

3) Cfr. V. Carlini, *Il lato oscuro dei listini: così gli algoritmi manipolano i mercati*, in *Il Sole 24 Ore*, 29 aprile 2018, su *https://www.ilsole24ore.com/art/il-lato-oscuro-listini-cosi-algoritmi-manipolano-mercati-AE1qK3eE*.

nario e dei derivati), sia del 50-70%[4]. 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 totale degli scambi conclusi, con una contrazione nell'ultimo anno di riferimento al 26%[5].

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

Ulteriore ambito è quello 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[6].

Vi è infine l'area che concerne la valutazione del merito creditizio, ossia la possibilità di concedere un determinato prestito, effettuata da un algoritmo sulla base delle informazioni raccolte.

3. *High frequency trading* – Rischi

Occorre soffermarsi sul fenomeno dell'HFT, per i rischi manipolativi che vi sono sottesi.

Le fattispecie manipolative possono infatti concretizzarsi attraverso il ricorso ad attività di trading basate sull'uso di algoritmi e programmi informatici ad "alta frequenza". Gli HFT sono veri e propri strumenti di intelligenza artificiale, capaci di apprendere dal contesto in cui operano e modificando di conseguenza le proprie strategie operative. Gli HFT sono dunque progettati per reagire alle variazioni del contesto in cui agiscono, senza la necessità di ricevere istruzioni aggiuntive rispetto a quelle inizialmente impartite dal programmatore "persona fisica".

---

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

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

6) 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*, in *Quaderni FinTech*, Consob, 6/2019, su *https://www.consob.it/documents/46180/46181/FinTech_6.pdf/185b-1db5-d48f-4bd9-864b-082e356cb992*.

Considerate le peculiarità che connotano tali strumenti, la loro rapida diffusione nel mercato e la sempre maggiore incidenza sui volumi di negoziazione si è sviluppata un'attenzione crescente riguardo agli stessi, soprattutto da parte delle Autorità di Vigilanza che si sono interrogate in merito ad eventuali rischi e conseguenze che ne possono derivare sui mercati. In particolare, i principali rischi connaturati all'utilizzo di HFT sono:

– rischi sistemici, in quanto eventuali malfunzionamenti di HFT possano essere emulati da altri HFT, con potenziali ripercussioni sull'intero mercato fino ad interessare anche altre *trading venue*s;

– rischi per la qualità del mercato in termini di efficienza informativa[7] e volatilità e liquidità del mercato[8].

3.1. Manipolazione di mercato – *Overview* generale

Come noto, esistono molteplici tecniche di manipolazione di mercato, alcune delle quali risalenti nel tempo, che l'utilizzo di avanzate tecnologie ha reso molto più complesse da individuare e più efficaci nei risultati. Tra queste tecniche meritano di essere evidenziate: spoofing, pump and dump, wash trading, bear reading, front running.

3.2. Manipolazione di mercato – Esempi di manipolazione operativa e informativa e casi pratici

Vengono di seguito riportate talune tecniche di attacco e difesa, relative a principali casistiche di manipolazione del mercato. In particolare, è descritto il processo relativo a quella specifica tecnica, con l'indicazione della tecnologia utilizzata. Infine, per ogni tecnica, viene riportato un caso pratico.

– *Spoofing*, Attacco: come viene manipolato il mercato.

L'operazione consiste nell'immettere sul mercato un ampio flusso di proposte di negoziazione. L'obiettivo non è concludere l'operazione, ma ge-

7) Il rischio di compromettere il corretto processo di formazione dei prezzi deriva dal fatto che ordini generati automaticamente non rappresentano un patrimonio informativo cui poter attingere per studiare i fondamentali economici del titolo negoziato, non veicolando informazioni in ordine al valore intrinseco dei titoli oggetto di scambio o all'andamento del mercato. Il proliferare di tale pratica potrebbe determinare un allontanamento dei prezzi di mercato dai fondamentali economici sottostanti riducendone il valore segnaletico. Inoltre, tale *modus operandi* potrebbe indurre gli operatori a prediligere piattaforme di negoziazione meno trasparenti (c.d. *Dark pools*) e ad allontanarsi dal mercato istituzionale.

8) L'HFT può, infatti, rappresentare una pratica che si sviluppa maggiormente in situazioni di elevata volatilità e che in seguito diventa essa stessa elemento che determina un'amplificazione dei movimenti anomali dei prezzi.

nerare informazioni fittizie per orientare le contrattazioni. Un'azione di spoofing viene perpetrata solitamente tramite l'utilizzo in mala fede dell'High Frequency Trading in quanto punta a turbare o destabilizzare i mercati, servendosi di sofisticati strumenti software/hardware, con i quali mettere in atto negoziazioni ad alta frequenza/velocità, guidate da algoritmi matematici.

– *Spoofing*, Difesa: come proteggersi.

Il modo migliore per proteggersi dallo Spoofing è adottare misure preventive che impediscano di essere vittima di manipolazione. Per prima cosa, essendo lo spoofing una tattica puramente a breve termine, si può evitare investendo a lungo termine ed evitando di effettuare transazioni quotidiane. Un'altra misura importante da adottare è quella di evitare di fare trading sugli exchanges sospetti. Dal punto di vista tecnologico, sono disponibili piattaforme in grado di identificare possibili azioni di spoofing tramite rilevazione di specifici ed avanzati pattern di Intelligenza Artificiale, analizzando le singole operazioni effettuate sui mercati.

– *Spoofing*, Un caso pratico.

Il 6 maggio 2010, un evento eccezionale si manifestò sui mercati. La giornata era partita normalmente, con dei leggeri ribassi veicolati da cattive notizie sul diffondersi della crisi greca nella zona euro. Alle 14.42, ci fu però un crollo improvviso degli indici americani, che persero il 10% in pochi secondi, in modo inspiegabile. Il delirio durò solo pochi minuti, in quanto in modo altrettanto inspiegabile quel flash crash si sistemò da solo, e i prezzi tornarono subito a livelli normali. Si scoprì che ad aver creato quel fenomeno fu una sola persona: Navinder Singh Sarao. Il trader manipolò il mercato piazzando e poi cancellando un ordine al ribasso di 200 milioni. Questo scatenò la reazione degli algoritmi automatici di trading, che iniziarono a loro volta a vendere senza sosta.

– *Pump and Dump*, Attacco: come viene manipolato il mercato.

La tecnica consiste nel diffondere notizie con cui si fa riferimento a titoli azionari appetibili dal punto di vista della redditività, acquistando in anticipo i titoli. L'incauto investitore una volta valutato il rumor acquista il titolo spingendolo ulteriormente al rialzo. Non appena i truffatori vedono aumentare le quotazioni del titolo per effetto degli acquisti, vendono traendone profitto. Tale tecnica può essere applicata attraverso telefonate/mailing/messaggi/post/chat, ecc.

– *Pump and Dump*, Difesa: come proteggersi.

Le comunicazioni sono inviate agli utenti da spammer professionisti che sanno bene come ottimizzare l'impatto dello spamming. È , quindi, necessario difendersi di conseguenza attraverso metodologie avanzate di Cyber

Security. Inoltre, è fondamentale dotarsi di strumenti e tecniche di identificazione di schemi/pattern di Pump and Dump. Quanto descritto può essere applicato attraverso Filtri antispam per email/sms e Real-Time Detection di eventi Pump/Dump, utilizzando tecniche di Intelligenza Artificiale basata sul Deep Learning, attraverso le piattaforme di Market Surveillance Software.

– *Pump and Dump*, Un caso pratico (Radio Corporation of America).

Appena entrata in Borsa (nel 1921) la Radio Corporation of America (di seguito, "RCA") valeva poco più di 20 dollari ad azione. Negli anni '20 un gruppo di investitori, alcuni di RCA, acquistò azioni dell'azienda per 12,7 milioni di dollari. Questi diffusero a taluni quotidiani, in particolare al Wall Street Journal, informazioni fuorvianti, riguardo grandi investimenti e sviluppi per la società, al fine di gonfiarne il valore azionario. La domanda di titoli RCA portò RCA a valere circa 550 dollari ad azione nel 1929. Con la crisi, chi aveva spinto la sopravvalutazione dell'azienda aveva già iniziato a vendere le loro quote. Nel '29 molti investitori, in difficoltà, iniziarono infatti a vendere le loro quote causando un calo immediato del valore. Altri, iniziarono a richiedere informazioni più precise per decidere se tenere o vendere i titoli. Questo fece emergere l'inesistenza del progetto di sviluppo promesso, facendo crollare RCA a circa 10 dollari ad azione. Prima dello scandalo di RCA, non esistevano leggi contro il Pump and Dump, che saranno introdotte per la prima volta proprio per conseguenza di tale vicenda, nel 1934. Gli autori, pur avendo causato gravissimi danni economici agli investitori, non erano punibili secondo le norme vigenti negli anni '20.

– *Wash Trading*, Attacco: come viene manipolato il mercato.

Il Wash trading è un processo mediante il quale un trader acquista e vende un titolo con lo scopo di fornire informazioni fuorvianti al mercato. In alcune situazioni, le operazioni wash vengono eseguite da un trader e un broker che sono in collusione tra loro. Il wash trading è emerso proprio mentre si stava diffondendo il fenomeno dell'High Frequency Trading, attraverso piattaforme software dedicate.

– *Wash Trading*, Difesa: come proteggersi.

Quando si valuta un potenziale Wash Trading, in primo luogo, si determina se gli ordini opposti per lo stesso strumento negoziato in borsa sono stati eseguiti l'uno contro l'altro allo stesso tempo e prezzo. In tal caso, si verifica se entrambe le operazioni sono state effettuate dallo stesso trader (o da trader collegati/in collusione). Attraverso le piattaforme di Market Surveillance Software è possibile configurare il sistema per identificare possibili schemi/pattern di Wash Trading su un determinato titolo.

– *Wash Trading*, Un caso pratico (Lo scandalo Libor).

Lo scandalo Libor è legato ad una serie di azioni fraudolente collegate al Libor (London Inter-bank Offered Rate), un tasso di interesse medio calcolato attraverso la presentazione dei tassi di interesse da parte delle principali banche di tutto il mondo. Il Libor dovrebbe quindi rappresentare la valutazione dello stato di salute del sistema finanziario. Molti prodotti finanziari si basavano sul Libor come tasso di riferimento; quindi, la manipolazione degli invii utilizzata per calcolare tali tassi può avere effetti negativi significativi sui consumatori e sui mercati finanziari. I primi sospetti sulla possibile manipolazione del Libor da parte di Barclays risalgono al 2005. Tra gennaio 2005 e giugno 2009, i trader hanno deliberatamente presentato tassi di interesse artificialmente bassi o alti per forzare il Libor ad aumentare o diminuire, nel tentativo di sostenere le proprie attività. Nel settembre del 2007, i tassi d'interesse comunicati erano tra i più alti di quelli delle altre banche che partecipavano alla determinazione del valore del Libor, cosa che fece nascere i primi sospetti. Alcune e-mail tra i responsabili della banca inviate all'epoca confermarono la manipolazione. Tra le conseguenze di tali azioni vi è stata la sostituzione di tale indice (dal 1° gen 2022) con indici basati su operazioni effettivamente chiuse e non sulle stime.

– *Bear Raid*, Attacco: come viene manipolato il Mercato.

Un Bear Raid è un tipo di strategia del mercato azionario, in cui un trader (o un gruppo di trader) tenta di forzare il prezzo di un'azione al ribasso. Un "raid" al ribasso può essere fatto diffondendo voci negative sull'azienda target. Una volta che il prezzo raggiunge il prezzo target (al ribasso), verrà acquistato dal trader per trarne profitto. I trader potrebbero assumere loro stessi grandi posizioni short, manipolando il prezzo con l'ampio volume di vendite, attraverso gli strumenti tecnologici dell'High Frequency Trading.

– *Bear Raid*, Difesa: come proteggersi.

Prima del 2008, il mercato era regolamentato dall'Uptick Rule che imponeva che la vendita allo scoperto di un'azione fosse consentita solo in caso di rialzo. Affinché la regola fosse soddisfatta, lo short doveva essere a un prezzo superiore all'ultimo prezzo negoziato (o quando il movimento più recente tra i prezzi scambiati è stato al rialzo). Dopo la crisi del 2008 le autorità competenti monitorano/regolamentano i mercati con nuove regole similari atte a scongiurare eventi di Bear Raid. Attraverso strumenti tecnologici avanzati è possibile configurare la Real-Time Detection di eventi Bear Raid, utilizzando tecniche di Intelligenza Artificiale basate sul Deep Learning.

– *Bear Raid*, Un caso pratico (Citigroup).

Si ritiene che l'abrogazione della normativa c.d. "Uptick Rule" avvenuta nel luglio 2007 abbia reso più facile per i venditori allo scoperto intraprendere

incursioni al ribasso. Il collasso di importanti istituzioni finanziarie nel 2008 è attribuito in alcuni ambienti ad azioni di Bear Raid. Il 1/11/2007, Citigroup ha, ad esempio, registrato un insolito aumento del volume degli scambi e una diminuzione del prezzo. Questo calo ha coinciso con un aumento anomalo delle "azioni prese in prestito" per un valore di quasi 6 miliardi di dollari, la cui vendita è stata una grande frazione del volume totale degli scambi, che è stato quasi quattro volte il volume abituale, facendo scendere i prezzi di quasi il 7%. Un numero simile di azioni è stato restituito sei giorni dopo. Quando le azioni sono state restituite, erano scese del 20%. L'entità e la coincidenza del prestito e della restituzione sono la prova di uno sforzo per abbassare il prezzo delle azioni e ottenere un profitto, attraverso un Bear Raid.

– *Front Running*, Attacco: come viene manipolato il Mercato.

La tecnica sfrutta la posizione di asimmetria informativa in cui versa chi invia l'ordine di compravendita di un determinato strumento finanziario. Il broker sfrutta la conoscenza dell'ordinativo effettuato e immediatamente prima di immettere l'ordine sul mercato acquista, il titolo in questione (se l'ordinativo è di acquisto) o lo vende (in caso contrario), traendo profitto dall'aumento/diminuzione del prezzo. Viste le caratteristiche peculiari di tale tecnica, l'High Frequency Trading, attraverso piattaforme software dedicate, è lo strumento tecnologico maggiormente usato dai broker fraudolenti.

– *Front Running*, Difesa: come proteggersi.

Nel Front Running l'informazione privilegiata è l'asset più importante da proteggere e gli insider primari (coloro che sono a conoscenza dell'informazione in quanto partecipano alla formazione della stessa) e gli insider secondari (coloro che ne vengono a conoscenza in diverso modo) devono proteggerla secondo le metodologie previste dalle normative di riferimento. Sul mercato esistono diversi strumenti per la gestione delle informazioni privilegiate e la corretta tenuta dei registri insider. Inoltre, è possibile configurare i sistemi di Market Surveillance Software per identificare possibili schemi/pattern di Front Running su un determinato titolo.

– *Front Running*, Un caso pratico (Citadel Securities).

Citadel Securities, Broker di proprietà del miliardario Ken Griffin, ha negoziato azioni per conto proprio dal 2012 al 2014 ritardando contemporaneamente gli ordini dei clienti per le stesse azioni. Secondo l'Autorità di regolamentazione finanziaria (FINRA - Financial Industry Regulatory Authority di Washington DC), Citadel ha rimosso centinaia di migliaia di ordini di grandi dimensioni dai suoi processi di trading automatico, richiedendo che tali operazioni fossero eseguite manualmente da trader umani. Allo stesso tempo, Citadel "*ha negoziato per proprio conto dalla stessa parte del mercato a*

prezzi che avrebbero soddisfatto gli ordini", violando i propri obblighi nei confronti dei propri clienti. In un solo mese campione, la FINRA ha scoperto che Citadel aveva scambiato contro i propri clienti in quasi tre quarti degli ordini. Alla fine Citadel ha accettato di risarcire i propri clienti, oltre a subire una multa di $ 700.000, pur senza ammettere alcun illecito.

4. *Market Surveillance*

Per contrastare la criminalità informatica in ambito Market Abuse, è necessario implementare e gestire un processo strutturato, denominato Market Surveillance. Tale processo è generalmente strutturato in varie fasi, di seguito descritte.

Ogni fonte dati rilevante deve essere sorvegliata ed utilizzata da un software specifico, con l'obiettivo di analizzare ed identificare i potenziali schemi/pattern fraudolenti. La tecnologia a supporto di tale fase può prevedere l'integrazione dei tool di trading con i software di Market Surveillance, con lo scopo di correlare gli ordini aziendali con i dati di mercato nonché le news e le informazioni da sorgenti pubbliche.

Successivamente, vengono generati degli avvisi specifici agli operatori che si occupano di Market Surveillance. Tali avvisi vengono generati in base a potenziali tipi di abuso, attraverso algoritmi avanzati di intelligenza artificiale e machine learning e secondo le parametrizzazioni impostate dall'utilizzatore. Le funzionalità di intelligenza artificiale e machine learning adeguatamente parametrizzate e configurate consentono di rilevare potenziali manipolazioni del mercato nonché comportamenti anomali dei propri dipendenti.

Terminate le prime fasi, vengono ricostruiti i possibili scenari di abuso ed avviata l'investigazione necessaria. I software di Market Surveillance consentono ai team specialistici di ricostruire i comportamenti che hanno generato l'alert e di svolgere gli approfondimenti necessari per prevenire ed eventualmente mitigare il rischio di Market Abuse.

In base ai risultati dell'analisi, vengono quindi intraprese delle azioni ed i risultati devono essere documentati attraverso specifici report debitamente archiviati. I tool, tramite funzionalità di reportistica, forniscono gli strumenti necessari per indirizzare eventuali azioni di escalation in conformità con le normative applicabili.

I principali driver che indirizzano l'implementazione e la parametrizzazione di tali sistemi sono dati dalla regolamentazione delle autorità di vigilanza che fornisce orientamenti specifici e standard minimi di copertura

del rischio di incorrere in pratiche di abusi di mercato. Pertanto, è necessario assicurare la compliance interna a tale regolamentazione, anche attraverso la definizione di adeguate policy e procedure per proteggersi dai citati eventi.

Le principali soluzioni di mercato in tale ambito sono: Eflow, Nasdaq, SteelEye, Trading Technologies, Scila, IBM Surveillance Isight.

5. *High frequency trading* – Alcuni casi giurisprudenziali

– *Sentenza Sergey Aleynikov* (2011): Alenynikov, responsabile GoldmanSach delle piattaforme di scambi ad alta frequenza effettuati su mercati telematici USA è stato condannato a 97 mesi di carcere dal Tribunale di NY per il furto e la ricettazione di 'codici sorgente' riservati, che consentivano l'accesso alla piattaforma HFT utilizzata dalla banca per operazioni di negoziazione su mercati azionari e delle materie prime. A destare scalpore fu l'ammissione, da parte della banca stessa, del pericolo che quei codici avrebbero potuto essere usati non soltanto per danneggiare la società, ma per manipolare i mercati, confermando quindi per la prima volta che gli enti che si avvalgono dell'HFT sono in possesso di tecnologie a tutti gli effetti potenzialmente manipolative.

– *Sentenza Micael Coscia* (2016): Michael Coscia, direttore e proprietario della Panther Energy Trading LLC, una società di trading "high-frequency" con sede nel New Jersey, è stata la prima persona ad essere processata per spoofing. Condannato a 3 anni di carcere (sentenza confermata in appello) dal Tribunale di Chicago per aver guadagnato più di $ 1 milione manipolando i prezzi dell'oro e di altri futures su materie prime utilizzando strategie di trading generate da HFT. A fornire prove contro di lui durante il processo è stata la testimonianza resa da un programmatore di computer della Panther che ha accusato Coscia di aver dato istruzioni specifiche su come progettare i sistemi di HFT e su come "far girare gli algoritmi".

– *Patteggiamento Deutsche Bank, UBS e HSBC* (2018): i tre colossi bancari patteggiano $ 47 milioni per episodi di spoofing sul mercato dei metalli preziosi negli USA e sull'indice S&P (vedendo anche l'incriminazione di alcuni loro trader) a fronte delle violazioni accertate dalla Commodity Futures Trading Commission degli USA e dal Dipartimento di Giustizia USA. L'accusa mossa verso di loro è di aver piazzato sul mercato migliaia di ordini "falsi" per indurre altri partecipanti al mercato a negoziare a prezzi, quantità o tempi che altrimenti non avrebbero scambiato. La Corte di giustizia a valle della sentenza ha dichiarato che: "Comportamenti come questo rappresentano

un rischio significativo di erodere la fiducia nei mercati statunitensi e creano un campo di gioco ineguale per i trader e gli investitori legittimi".

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. 3.2, 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[9].

9) 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* (CAHAI), 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.*

Criptovalute ed attività criminali: ragioni di un dialogo interdisciplinare

di Fabio Di Vizio, Francesco Bruschi e Vincenzo Rana*

1. Premessa

Un seminario assai stimolante quello organizzato il 18 maggio 2022 dalla Fondazione Vittorio Occorsio per la Scuola di Perfezionamento per le Forze di Polizia intitolato "*Criptovalute ed attività criminali*" in seno al XXXVII Corso di Alta Formazione sulla "*Criminalità informatica ed intelligenza artificiale*".

L'apprezzamento espresso all'esito dell'incontro ha suggerito di replicare la formula didattica sperimentata, privilegiando l'esposizione dialogica seguita durante i lavori, giovandosi del sapere di studiosi ed esperti riconosciuti a livello nazionale. Seguendo tale ispirazione saranno riproposti i contenuti storici del dialogo coordinato dal dott. Fabio Di Vizio con la collaborazione dei professori Francesco Bruschi e Vincenzo Rana.

Nelle pagine dell'opera potranno rinvenirsi, con l'autenticità propria di un confronto svoltosi a voci vive, le nuove certezze acquisite, gli antichi dubbi, le effettive prospettive di indagine e la forte smitizzazione di ipotesi ricostruttive scisse dalla reale conoscenza del funzionamento di sistemi informatici, tecnologici ed economici in rapida evoluzione. Le puntuali domande dei discenti, incuriositi dalla materia e stimolati dai relatori, offrono la testimonianza più autentica del successo di questa modalità espositiva organizzata con sessioni *hands-on* che pongono ai partecipanti dinanzi ad esperienze pratiche.

Chi pensa di trovare nell'ecosistema delle criptovalute semplici declinazioni dell'anarchia, dell'individualismo e della disintermediazione sfrenata, potrà motivatamente ricredersi. Vengono offerti dati oggettivi che consentono di riconoscere come la "trasparenza tra i privati" stia diventando veicolo dell'aspirazione delle autorità centrali ad individuare nuove declinazioni del

(*) Fabio Di Vizio è Sostituto Procuratore della Direzione Distrettuale Antimafia presso la Procura di Firenze. Francesco Bruschi è laureato in Ingegneria Elettronica presso il Politecnico di Milano, dove ha anche conseguito il dottorato in Ingegneria dell'Informazione ed è attualmente docente di Sistemi di Elaborazione dell'Informazione; é inoltre direttore dell'Osservatorio Blockchain e Distributed Ledger Technologies, istituito presso il Politecnico di Milano. Vincenzo Rana è laureato in Ingegneria Informatica presso il Politecnico di Milano, dove ha conseguito il dottorato in Ingegneria dell'Informazione; é attualmente docente a contratto presso il Politecnico di Milano e ricercatore presso l'Osservatorio Blockchain e Distributed Ledger Technologies.

controllo pubblico; inoltre, al crescere della portata sistemica del settore, l'intermediazione, com'è inevitabile, torna ad espandersi e sollecita interventi normativi. Con la consapevolezza che la ricerca e la condivisione di un linguaggio comprensibile, puntuale e tecnicamente appropriato, sia la precondizione per governare con efficacia qualsiasi impegno investigativo, vivificato da innesti interdisciplinari connaturati ad una realtà complessa.

La democratizzazione, l'inclusione finanziaria e gli ulteriori vantaggi economici che hanno accompagnato lo sviluppo delle criptovalute e delle tecnologie ad esse sottese non possono indurre a trascurare i rischi di loro impieghi criminali e le esigenze di protezione da esse suscitate. La consapevolezza di queste ultime è destinata ad accrescersi con l'acquisizione della portata sistematica del settore e con la sua maggiore interazione con l'economia "reale". Le stesse ragioni dei dubbi sull'opportunità di dettare regole rispetto ad un processo innovativo in espansione vissuto nell'esaltazione della disintermediazione e dell'emancipazione dal controllo di autorità centrali e pubbliche sono venute smagrendosi difronte all'incremento dei poliedrici servizi di intermediazione connessi all'utilizzo delle valute virtuali, offerti da soggetti non provvisti di rassicuranti di requisiti patrimoniali rispetto alle risorse amministrate ed investite. In più, il proliferare di impieghi criminali favoriti dalle criptovalute impone una nuova consapevolezza degli strumenti preventivi, investigativi e giudiziari per contrastarne il successo e la diffusione.

Nel dialogo tra gli esperti è possibile rinvenire i contenuti completi, sia pur sintetici, di un corso di "*Istituzioni di tecnologia e di diritto delle criptovalute*".

Si principia con l'esame lucido dei profili tecnologici, informatici e crittografici, imprescindibili, in particolare, per l'analisi approfondita delle innovative infrastrutture che hanno consentito la diffusione delle criptovalute e che si pongono come straordinarie novità tecnologiche, suscettibili di impieghi che meritano l'interesse degli intermediari tradizionali e delle autorità di settore.

Dal funzionamento dell'ecosistema delle criptovalute, l'esame viene trasferendosi sui diversi approcci normativi. Dopo un quadro comparativo, l'attenzione è stata riservata alle diverse impostazioni sinora seguite dalle Autorità di settore sino ai risultati degli sforzi, affatto esauriti, operati dai decisori politici e dalla riflessione giuridica per offrire conveniente inquadramento dogmatico a uno strumento che nasce fuori della regolazione pubblica e che riferisce non poco del proprio valore alla condizione di anomia. Sono state ripercorse, quindi, in breve, le diverse esperienze di normazione, sviluppatesi lungo la direttrice del presidio delle aree di diretta interferenza delle valute

virtuali con le monete correnti e l'economia reale: un'immaginifica "cinta daziaria" dotata di porte per individuare chi e che cosa passa dal mondo reale a quello virtuale.

Il ruolo del presidio penale si è venuto profilando come affatto trascurabile nella gestione della salvaguardia di moderne esigenze di protezione scaturenti dall'innovativo valore digitale; ha trovato spiegazione la ragione autentica per cui l'originale fenomeno tecnologico sotteso alle criptovalute ne favorisce possibili interferenze con aree criminali, capaci di strumentalizzarne le caratteristiche, sfruttando le vaste opacità.

Le indagini devono acquisire la lucida maturità di modellarsi sul loro oggetto, calibrandosi su una realtà "virtuale" nuova, senza figurarsene una tradizionale immaginaria che finirebbe per segnarne l'irrimediabile insuccesso.

Oltre al quadro dei reati connessi all'utilizzo delle criptovalute, trova approfondimento, durante una straordinaria esperienza laboratoriale nella sessione *hands-on* – unica nel genere – l'analisi delle principali criticità cui si espone l'efficacia delle indagini rispetto a reati coinvolgenti l'impiego di criptovalute, quelli cioè 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. Particolari approfondimenti sono stati dedicati, infine, alle problematiche connesse all'eseguibilità dei sequestri di criptovalute da parte delle forze di polizia e dell'Autorità giudiziaria.

2. Inquadramento tecnologico e giuridico

Dott. Fabio Di Vizio: Buongiorno a tutti. Anzitutto, vi ringrazio per questo confronto che, devo dirlo, costituisce occasione formativa anche per me. Dovendo preparare la sessione ho immaginato di offrirvi una serie di stimoli; poi, nel programmarli mi sono accorto che la riflessione da proporvi doveva farsi necessariamente più profonda, uscendo dal dato puramente tecnico-giuridico, espandendosi alla dimensione economico-sociale.

La materia che ci impegna è quella delle criptovalute e dei loro rapporti con le attività criminali. Non vorrei farvi accostare a queste tematiche secondo un'impostazione necessariamente negativa ovvero diffidente. Naturalmente ci occuperemo di aspetti di interesse criminale perché è indubbia una stretta e sperimentata connessione con una serie di reati, dal riciclaggio a forme di abusivismo sino ad altre figure criminose che ripercorreremo e, per lo

più, potremo sono accennare; però, l'approccio che vorrei cercare di proporvi è di chi guarda al nuovo fenomeno con attenzione vigile, che non demonizza e non mitizza. In particolare, non demonizza quella che costituisce la base tecnologica, sempre più apprezzata, ancorché in fase di sperimentazione; non mitizza neppure i profili normalmente individuati come caratteristici. Penso, a tal proposito, alla disintermediazione e alla decentralizzazione: il tema, in buona sostanza, della possibilità di affrancare il controllo e l'impiego delle valute dal Governo e dal controllo delle autorità centrali.

Anzitutto, venendo più direttamente all'organizzazione della sessione, la prima parte, di circa un'ora, sarà dedicata ai profili tecnologici, informatici e crittografici: cioè, cercheremo di capire, con il prezioso contributo con due professori del Politecnico di Milano, quali siano le infrastrutture informatiche e crittografiche che hanno consentito la diffusione delle criptovalute, ponendosi anche quale occasione di sviluppo dei servizi dei cosiddetti intermediari tradizionali. Questa prima sessione, vedrete, è essenziale e sarà assolutamente utile a chiarire premesse e diradare dubbi; perciò, ho invitato i due correlatori ad illustrare i temi loro affidati con un linguaggio accessibile a chi ha normalmente alle spalle studi giuridici, evitando di semplificare troppo, ma senza rendere troppo complicato quello che si deve ben comprendere per ben gestire le indagini.

La seconda sessione sarà dedicata all'inquadramento normativo di questo fenomeno particolarissimo. Qualcuno ha scritto di un moderno ircocervo, altri hanno parlato di un attivo senza un passivo; qualcuno vi intravede un clamoroso vizio di origine e una fragile ricchezza malata che viene dal nulla. Mi permetto di dire subito qualcosa su questo argomento; se questa è la debolezza del valore peculiare che stiamo per esaminare allora qualche ragione sistematica di fragilità deve riconoscersi anche alle base del governo delle valute tradizionali. La logica convenzionale, infatti, è quella che ne sostiene il valore, almeno dagli accordi del 1971, quando fu sospesa la convertibilità del dollaro in oro. Singolarmente questo avvenne per esigenze belliche, bisognava finanziare la guerra del Vietnam. Il fatto che alla moneta non corrisponda necessariamente un valore collaterale, dunque, è già realtà, per quanto in parte dimenticata e quasi inconsapevole, della nostra vita quotidiana. La differenza è che in quest'ultima ci sono autorità centrali capaci di mitigare la componente virtuale del valore della moneta; diversamente, nel mondo delle criptovalute la virtualità è senza mediazioni, vorrei dire "tangibile", in quanto gestita dagli utenti e dagli altri soggetti caratteristici dell'ecosistema.

Un'ulteriore porzione di questa progettata frammentazione dei lavori, è dedicata alle attività criminali, cioè ai profili di possibile strumentalità crimi-

nosa delle criptovalute, accennando all'inquadramento che ne offre il Codice penale e l'ulteriore legislazione penale. L'ultima porzione, infine, è incentrata su un'esperienza laboratoriale, che consentirà ai partecipanti di mettere "le mani in pasta". Immagino che sia la parte più attesa, foriera di dubbi ma spero anche utile a stimolare domande per risolverli. Cercheremo di guidarla seguendo due direttrici: che cosa si può fare per identificare i soggetti che controllano i portafogli, o comunque le criptovalute? E che cosa si può fare per assumere concrete iniziative di congelamento piuttosto che di sequestro rispetto a questi valori sostenuti, se non costituiti, da strutture informatiche? Senza tacere i difetti e le potenzialità delle diverse soluzioni.

Passo ora la parola al Professor Francesco Bruschi, direttore dell'Osservatorio *blockchain* istituito presso il Politecnico di Milano, e al Professor Vincenzo Rana, ricercatore presso lo stesso Istituto Universitario. Affido a loro, quindi, una breve introduzione entro il solco sin qui molto brevemente tracciato.

Prof. francesco Bruschi: Buongiorno a tutti, grazie per l'introduzione. Sono molto contento di essere qui con voi. C'è un po' di rammarico nel non essere in presenza, purtroppo logisticamente la cosa era molto complicata. Come è stato anticipato, io mi occupo di queste questioni come docente del Politecnico di Milano, e come direttore dell'Osservatorio del Politecnico di Milano. All'Osservatorio osserviamo appunto, come si può intuire dal nome, queste tecnologie e le loro opportunità in ambito finanziario e in ambito economico, ma scrutiamo anche da vicino (io sono un ingegnere elettronico informatico) i presupposti tecnici e le prospettive tecnologiche, che cosa si può fare, che cosa non si può fare e quindi abbiamo questo polso e speriamo questa sensibilità che oggi vorremmo provare a trasmettervi. Presento anche il mio collega e amico Vincenzo Rana. Anche Vincenzo è un docente del Politecnico ed è anche lui un ricercatore dell'Osservatorio

Prof. Vincenzo Rana: Eh sì, buongiorno a tutti. Francesco, hai già introdotto molto bene che cosa facciamo riguardo a tematiche interessanti, un po' tecniche, quindi cercheremo di renderle comunque fruibili. Vedremo poi come farvi anche interagire sia nella parte di spiegazione, sia in quella un po' più pratica.

Prof. francesco Bruschi: Va bene, grazie Vincenzo. Come ha anticipato, adesso mi prenderò un po' di tempo per cercare di introdurvi a qualche elemento, sia tecnico ma anche storico, se vogliamo anche culturale, in merito al contesto di questi strumenti. Quindi vi "infliggerò" questa oretta di teoria ma non vi preoccupate perché alla fine della mattinata è prevista una sessione *hands-on* in cui vi chiederemo, se vorrete, di mettere in pratica insieme a noi

molte delle cose che vedremo in questa prima parte. Allora io procedo subito condividendo lo schermo, ho qualche slide che mi aiuta a tenere il punto.

L'idea è di far comprendere da dove originano questi principi tecnici e poi di parlare delle applicazioni, perché, come ha detto il dottor Di Vizio, è vero che queste tecnologie spesso salgono alla ribalta per fatti non piacevolissimi però, in realtà, quello che offrono sono anche possibilità applicative estremamente interessanti e di questo spero di darvi qualche prova. Ora possiamo partire.

Ci sono moltissimi modi per introdurre la questione. Io vi propongo un approccio storico, ricordando: da dove nascono le tecnologie *blockchain* e le criptovalute? Quale problema intendevano risolvere i loro inventori? Uno dei punti di ingresso è sicuramente questo: il movimento *cypherpunk*, movimento di attivisti della privacy e appassionati di crittografia, verso la fine degli anni '90 del secolo scorso, voleva creare qualcosa di ambizioso, cioè il denaro digitale e "liberamente" scambiabile tra i soggetti. Che cosa intendiamo con "liberamente"? Per darvi un'idea, poniamoci in quel contesto e ricordiamo che da ormai qualche anno era disponibile a tutti una tecnologia che si era diffusa ampiamente, ovvero quella di *Internet*, che consentiva, con modalità nuove per la storia dell'umanità, di trasferire in maniera libera informazioni tra soggetti qualsiasi sul pianeta. In effetti, quindi, qualsiasi soggetto, grazie ad Internet, poteva già negli anni '90 scambiarsi delle informazioni senza dover ricorrere ad attori istituzionali o a garanti di questo scambio di informazioni. In che modo? Sappiamo ormai (è nella nostra esperienza quotidiana) che l'insieme degli attori che si scambiano informazioni su Internet è una rete decentralizzata, estremamente difficile da controllare, nel senso che è difficile prevenire il fatto che due persone si possono scambiare informazioni. L'*email* è un esempio tipico. Se l'informazione poteva essere scambiata liberamente, il "valore" ancora no. Perciò mandare un messaggio da un soggetto a un altro era liberalizzato grazie a Internet, mandare del valore (poi vediamo cosa intendiamo col valore) invece no. L'ambizione di questi appassionati di crittografia era creare un meccanismo che consentisse di fare con il valore ciò che si faceva già con l'informazione.

Che cosa intendiamo con "liberamente"? Quale era l'obiettivo ideale di questi *cypherpunk*? Possiamo descriverlo (e viene descritto anche nell'articolo seminale che poi vedremo dopo, che dà un po' origine a tutte queste tecnologie): l'obiettivo o l'ispirazione è quella del contante come modello per il trasferimento di valore. Ora noi sappiamo che il contante ha caratteristiche peculiari interessanti: in particolare, è custodibile e trasferibile senza richiedere collaborazioni di terze parti. Quindi io ho 10 € in tasca, posseggo

questi 10 € in virtù del fatto che ho una tasca che contiene questa banconota; se voglio trasferirli, ammesso che si sia prossimi alla persona, li passo e non è richiesta la collaborazione di nessun altro se non di chi riceve e intasca questa banconota.

Ecco, invece, qualcuno potrebbe obiettare che il denaro digitale lo avevamo già negli anni '90: le carte di credito con cui facciamo trasferimenti digitali, con cui compriamo su Internet. È assolutamente vero. Però faccio notare un paio di particolarità e di requisiti per l'utilizzo di questo denaro. In tutti i trasferimenti (un bonifico elettronico, un trasferimento tramite carta di credito) serve sempre la collaborazione di un soggetto terzo: una Banca, un operatore di pagamento, un altro soggetto. Se voglio trasferire quegli stessi 10 € in formato digitale, questo trasferimento richiede necessariamente che un attore dia del supporto attivo. Se questo attore in qualche modo questo supporto lo nega, per mille ragioni, il trasferimento non può avere luogo. Inoltre, tipicamente c'è identificazione di tutti i trasferimenti. Questo era percepito come un limite da parte dei nostri amici *cypherpunk*.

Cosa vorrei provare a fare adesso? Mettiamoci nei panni e nella prospettiva culturale di questi attivisti e vediamo come si può provare a realizzare un sistema di trasferimento del valore digitale che si avvicini di più al contante e consenta di trasferire il valore fra soggetti senza richiedere l'identificazione e senza richiedere la collaborazione attiva di un soggetto terzo. Quindi questo è un po' quello che vi chiedo di fare, ovvero di metterci nei panni di questi signori e provare a tendere a questo obiettivo.

Allora, vi propongo qualche ingrediente tecnico. Che cosa ci serve per realizzare un sistema con il quale possiamo trasmettere qualcosa? Immaginiamo di voler rappresentare degli oggetti digitali che creiamo in forma finita. Possiamo immaginare di voler creare *voucher* con il quale ci scambiamo dei servizi (questo è un esempio reale, tra l'altro) all'interno di una cooperativa di famiglie, per esempio di *babysitting* (e qua mi rifaccio sempre a un caso reale, studio anche di alcuni economisti); vogliamo creare una serie di oggetti che ci potremmo scambiare senza chiedere il permesso a nessuno. Che cosa serve per fare una cosa del genere?

Servono sostanzialmente tre cose: una rappresentazione di chi ha che cosa, quindi del possesso di questi oggetti o di questi *asset*; le regole con cui possiamo aggiornare la nostra rappresentazione; inizialmente, un amministratore che gestisca la rappresentazione ed esegua le regole. Per quanto riguarda la rappresentazione non pensate a qualcosa di complicatissimo, in realtà è qualcosa di estremamente semplice: può essere tranquillamente una tabella a due colonne (poi vi faccio un esempio in una slide successiva) in cui viene de-

scritto chi ha che cosa, quindi avremo due colonne; nella prima colonna sarà rappresentato un soggetto che detiene del valore o degli asset, nella seconda colonna rappresenteremo quanti asset questo soggetto detiene. Le regole con cui questa rappresentazione può evolvere sono altrettanto semplici: il titolare di una riga (quindi se appunto io sono alla terza riga, c'è il mio nome, c'è scritto quanti asset ho) può disporre di trasferire questi asset (quindi posso e voglio dare questi due asset al Dottor Di Vizio, questo è possibile farlo, a patto che il saldo indicato sulla tabella sia effettivamente superiore a due e che io ovviamente sia stato identificato). Questo è ancora più semplice se lo rappresentiamo. Vedete questa possibile rappresentazione: qua abbiamo una tabella che rappresenta degli oggetti digitali, dei voucher. In questo caso sono 30. Ok, perché immaginiamo che questa sia tutta la tabella.

Mario Rossi	10
Stefano Bianchi	15
Giuseppe Verdi	5
…	

Qui abbiamo una rappresentazione di 30 asset digitali distribuiti in questo modo. L'amministratore è colui che esegue le regole. Se Mario Rossi vuole trasferire due dei suoi *voucher* a Stefano Bianchi come funziona? Mario Rossi si fa riconoscere dall'amministratore, esprime il suo mandato e la sua volontà di trasferimento; l'amministratore identifica Mario Rossi e poi procede a modificare le righe della tabella. Di conseguenza, il 10 diventa 8, il 15 diventa 17. Ora in questa modalità, credo che qua non ci sia niente di misterioso o di oscuro, questa è una prima possibilità con cui possiamo implementare la contabilità. È molto simile a quello che fa la nostra Banca che ha una tabella che contiene esattamente queste informazioni.

Questo soddisfa i nostri *cypherpunk*? Ovviamente no, perché ci sono diversi limiti. Prima di tutto qui è necessario affidarsi a identità anagrafiche, quindi l'amministratore deve riconoscere, anzitutto, i soggetti e per farlo deve "appoggiarsi" a qualche meccanismo di identificazione: questo può avvenire tramite un documento d'identità oppure digitalmente – potremmo utilizzare

qualche infrastruttura come SPID – e poi deve attivamente eseguire il trasferimento degli asset operando sulla tabella. Questo meccanismo è lontano dall'essere libero in quella accezione ideale di cui si diceva prima. Vediamo come possiamo andare nella direzione di una maggiore libertà, come possiamo andare verso le proprietà tipiche del contante.

La prima cosa che potremmo fare è risolvere la questione delle identità reali: potremmo introdurre la pseudonimia, ma in che modo? La soluzione è abbastanza semplice, la sperimentiamo quotidianamente accedendo a servizi informatici: invece di rappresentare gli utenti tramite la loro identità anagrafica ufficiale, li rappresentiamo tramite pseudonimi che normalmente chiamiamo *username*. Nella tabella abbiamo sostituito i nomi con *username* e le regole rimangono quelle. Se controllo lo *username* "Pippo" e voglio trasferire parte dei miei *asset*, quello che devo fare sarà farmi identificare dall'amministratore, dopodiché quest'ultimo procederà a eseguire il mio mandato. Ecco cosa succede in questo caso: l'amministratore non può più contare sul documento d'identità, quindi occorre un altro meccanismo di identificazione. Non è un problema, ci sono diverse soluzioni. Quella più classica la conosciamo ormai da decenni: si basa sulla condivisione di un segreto con l'amministratore. In un momento iniziale mi registro presso il servizio, comunico il mio *username* che l'amministratore controlla che non sia già usato da qualcun altro, comunico all'amministratore un segreto, ovvero la *password*, e l'amministratore memorizza il segreto che gli ho comunicato. Poi successivamente, quando mi voglio identificare come "Pippo", l'amministratore mi chiederà di dimostrarlo comunicandogli il segreto convenuto; a quel punto lui mi ha autenticato e può eseguire il mio mandato. Questo sistema, che conosciamo assolutamente tutti, funziona.

Attenzione, però: questo sistema ha limiti. Infatti, anche se le *password* non vengono memorizzate dall'amministratore in chiaro ma attraverso tecnologie crittografiche che ne rendono la memorizzazione più sicura, l'amministratore continua a essere necessario se non fosse altro per il fatto che è colui che deve conoscere le *password*, deve memorizzarle, deve tenere il segreto e procedere all'identificazione.

C'è però un altro problema. L'amministratore ha un potere estremamente forte che è questo: idealmente può disporre trasferimenti arbitrari. Ad esempio, se io sono Pippo e a un certo punto invece che 10 voucher come mi aspetto me ne trovo 8, che cosa faccio? Posso contestare il fatto che mi sono stati tolti due *voucher* per i quali non ho dato mandato di trasferimento. A questo punto però è la mia parola contro quella dell'amministratore; quest'ultimo può dire "*ma certo che tu mi hai dato mandato di trasferire questi ogget-*

ti, non ti ricordi? Mi hai chiamato il giorno X e mi hai detto la tua password". Questo è un punto su cui vorrei porre una forte attenzione. In un sistema come questo, l'amministratore ha il potere di fare un trasferimento arbitrario e in quel caso è molto difficile per un utente dimostrare che non c'è stato un mandato di trasferimento: è la parola dell'utente contro quella dell'amministratore. L'amministratore non richiede una prova opponibile del fatto che ha ricevuto effettivamente un mandato: questo succede con la Banca ma non ce ne preoccupiamo, perché è un soggetto di cui ci fidiamo. Nella nostra prospettiva stiamo cercando di eliminare la necessità di attori dei quali ci fidiamo. Ad esempio, ci fidiamo del fatto che la banca non ci prelievi arbitrariamente gli euro e li trasferisca da qualche altra parte. Ci fidiamo per ragioni però che non sono tecniche, sono estrinseche al meccanismo tecnico. Qui vorremmo fare qualcosa di più, vorremmo riconfigurare il sistema in modo che l'amministratore non possa proprio farlo. E non perché sia "bravo", ma per ragioni tecniche. Come si fa? Qui si realizza il primo grande salto: lo possiamo fare utilizzando la tecnologia che non è nuova, che esiste da molto tempo, però la impieghiamo in un modo innovativo: la tecnologia delle firme crittografiche.

Le firme crittografiche funzionano attraverso una serie di strumenti tecnici che vanno sotto il nome di crittografia asimmetrica. In estrema sintesi, è un sistema all'interno del quale chiunque può generare una coppia di chiavi. Cosa sono le chiavi? Immaginatele tranquillamente come numeri molto grandi. Adesso posso generare in totale autonomia una coppia di chiavi: una la chiamo pubblica e una privata. La chiave privata che posso generare è unica, l'avrò soltanto io. Come faccio a generare una chiave autonomamente, che non ha nessun altro? È molto semplice, sostanzialmente si tratta di generare un numero casuale sufficientemente grande. Per esempio, se lancio un dado 100 volte e compongo tutti gli esiti, mi verrà un numero molto lungo per cui la probabilità che sia lo stesso numero che ottiene qualcun altro è infinitesima. In genere sono una coppia di chiavi, una privata, che devo tenere nascosto e una che è strettamente collegata che invece è pubblica e posso, anzi devo diffondere e trasmettere a più persone possibili. Cosa è possibile fare grazie alla crittografia asimmetrica con queste due chiavi? Una cosa estremamente interessante: dato un messaggio, è possibile, conoscendo la chiave privata, creare una firma di quel messaggio a nome della chiave pubblica e questa firma ha proprietà interessanti, la più notevole delle quali è che chiunque altro può verificare, dato il messaggio e data la firma, che quest'ultima è stata generata necessariamente da qualcuno che conosce la chiave privata. Ho spiegato in estrema sintesi il funzionamento delle firme crittografiche.

Le firme crittografiche, quindi, consentono di creare le prove digitali di

provenienza di un messaggio. Questo meccanismo, per quanto semplificato, è esattamente quello alla base delle firme digitali che oggi hanno valore legale e che ormai utilizziamo sempre più frequentemente.

Come utilizzo le firme crittografiche in questo contesto? Qui abbiamo fatto l'80% del salto che catapulta dentro le criptovalute. Mentre prima avevo rappresentato gli utenti tramite lo *username* e la *password*, adesso gli utenti li rappresenterò tramite le loro chiavi pubbliche. Cioè io sono un soggetto che vuole entrare in questo sistema perché voglio ricevere dei *voucher*, quello che farò sarà generare questa coppia di chiavi in totale autonomia, dopodiché pubblicherò la mia chiave pubblica che funzionerà come un identificativo della mia riga: potete tranquillamente immaginarlo come un codice Iban. A questo punto il ruolo dell'amministratore muta sostanzialmente, perché quando voglio trasferire dei voucher che posseggo ciò che devo fare sostanzialmente è creare un messaggio, un mandato del tutto equivalente a un assegno. In questo assegno scrivo: da chi proviene il trasferimento, a chi s'intende trasferire i *voucher*, quanti ne devo trasferire e poi una firma digitale con la quale chiunque può verificare che tutto questo assegno è stato effettivamente generato dal proprietario o dal controllore di questa chiave pubblica, in virtù della sua conoscenza della chiave privata. Nell'esempio di prima questo potrebbe essere Pippo che si è creato una chiave pubblica e quindi a questo punto viene rappresentato nella contabilità attraverso la sua chiave pubblica.

Dott. Fabio Di Vizio: non voglio interromperla ma intendevo sottolineare che, destrutturando l'analisi classica, Lei ci sta accompagnando in una ricostruzione delle modalità con le quali si elimina il controllo dell'amministratore rispetto alla risorsa.

Prof. francesco Bruschi: siamo partiti dalla visione nota della gestione degli *asset*, quella in cui un soggetto è investito della responsabilità della contabilità. Pian piano ne stiamo ridimensionando le prerogative perché vogliamo creare un sistema nel quale non è richiesta la fiducia nel comportamento onesto dell'amministratore, del quale miriamo a comprimere il ruolo. In questo caso quando io voglio mandare dei *voucher* a qualcun altro firmo un assegno e lo trasferisco all'amministratore. L'amministratore, a questo punto pubblica questo assegno, questa transazione che chiunque può vedere e quindi lui non può più disporre trasferimenti arbitrari, perché nel momento in cui vedessi che mi mancano dei *voucher* potrei fargli questa obiezione "*quando ti avrei detto di trasferire questi voucher?*"; l'amministratore dovrebbe produrre una prova del trasferimento del mio mandato che dovrebbe essere un assegno firmato da me, ma ovviamente, siccome grazie alla crittografia lui non può falsificare la mia firma non potrebbe dimostrare questa cosa e quindi non c'è

bisogno di fidarsi del fatto che lui non trasferirà arbitrariamente perché non lo può più fare. In altri termini, qui il ruolo dell'amministratore diventa quello di un passacarte: deve soltanto prendere questi mandati, verificare le firme e poi pubblicarli. Se noi immaginiamo di avere a disposizione tutto l'elenco dei mandati di trasferimento dall'inizio del funzionamento del sistema, in realtà chiunque può verificare in ogni momento che l'attuale situazione contabile effettivamente è corretta. So che inizialmente i miei tre partecipanti avevano 10 *voucher* ciascuno, è corretta questa situazione contabile attuale? Se voglio verificarlo vado a ripercorrere la storia di tutti i trasferimenti, vedo che cosa mi viene fuori e verifico se il risultato è congruente con quello rappresentato dall'amministratore. Si potrebbe anche dire che in questa rappresentazione "contabilizzata" l'amministratore non serve più. Chiunque può vedere in ogni momento, percorrendo l'effetto delle transazioni qual è lo stato attuale. Quindi l'amministratore ha solo un compito, ricevere le transazioni e rappresentarle in una lista che tutti possono vedere. Questa costituisce veramente un'estrema compressione delle prerogative dell'amministratore. Se ci sono domande, ci sono dubbi, non fatevi alcuno scrupolo a interrompermi.

PARTECIPANTE AL SEMINARIO: Premetto che per me è una materia abbastanza ostica, quindi la mia domanda potrebbe essere anche forse troppo semplicistica, ma alla fine, dal discorso che lei ha fatto in maniera molto chiara per comprendere proprio i passaggi per i quali si fa a meno dell'intermediario, però alla fine mi sembra che l'intermediario ci sia, cioè è la stessa cosa che facciamo con la banca, perché anche la banca ha bisogno delle nostre credenziali per trasferire i nostri valori. Cosa cambia rispetto al meccanismo che noi normalmente sperimentiamo con le banche?

PROF. FRANCESCO BRUSCHI: Grazie, è una domanda tutt'altro che semplicistica. Anzitutto devo premettere che non abbiamo ancora concluso il nostro viaggio verso la decentralizzazione. Però si può già evidenziare una differenza: quando noi ci colleghiamo con la banca, come dicevo prima, diamo un mandato per un bonifico di trasferimento. Ci colleghiamo e diciamo "sono Francesco Bruschi"; "qual è la tua *password*"? Comunico la mia *password* e poi un secondo codice che dimostra altre cose. Ad un certo punto, la banca è convinta che io sia Francesco Bruschi e quando io do un mandato di trasferimento, la banca lo esegue, è tutto a posto. Attenzione: quello che mettevo in evidenza è che in questo procedimento c'è un elemento di forte fiducia nel fatto che la banca esegue soltanto i trasferimenti per i quali ha ricevuto mandato. Questo problema, per lo più, non lo avvertiamo perché tutto il nostro sistema garantisce molto bene che le banche si comportino correttamente. Ci fidiamo del fatto che la Banca faccia questo perché ha una serie di vincoli a

farlo per tutta una serie di ragioni. Qui però ci stiamo ponendo una questione un po' diversa ed è se questa responsabilità la concederemmo mettendoci nelle mani di uno sconosciuto. Investiremmo con un soggetto che non è vigilato, non vincolato come una banca a gestire i nostri risparmi? Probabilmente no. Perché? Perché, appunto, questo soggetto potrebbe dire "*guarda tu mi avevi detto di fare un trasferimento*": in realtà voi invece non l'avete detto e tecnicamente non c'è modo di risolvere questa disputa. Questo è un fatto. Poi, noi non lo consideriamo perché le banche non si comportano così.

Dott. Fabio Di Vizio: La questione è chi controlla direttamente la risorsa al momento del trasferimento. Come ricordava il professor Bruschi, questa elaborazione, *Bitcoin*, nasce nel 2009. Non è casuale il 2009, è l'anno che segue i famosi scandali delle banche americane, a seguito dei quali i risparmiatori avevano scoperto amaramente che le risorse che ritenevano di avere in realtà non c'erano più. E ciò perché c'era stato il loro impiego nei mutui *subprime*, le sovvenzioni concesse con criteri assolutamente poco prudenziali sul versante della stabilità degli istituti bancari. Questo offre la spiegazione dell'esigenza per cui il "mio" risparmio, la "mia" risorsa, devo poterla controllare "io" fino in fondo, senza affidarne il trasferimento a qualcun altro. La chiave è quella firma, che determina, a tutti gli effetti, il trasferimento giuridico.

partecipante al seminario: Grazie per la concretezza dell'intervento. Io volevo chiedere una cosa, sono sul sito *blockchain.com* dove sto vedendo una serie di transazioni che si susseguono, giusto per capire se sono quelle le transazioni di cui parliamo. Hanno dei codici crittografici, come quelli che lei ci sta mostrando. Mi ricollego all'osservazione della collega: mi devo fidare in qualche modo che sono vere quelle transazioni? Cioè c'è un controllore del sito?

Prof. francesco Bruschi: Grazie per la domanda che tocca diverse dimensioni. Adesso proseguo sulla decentralizzazione. Dopo aver compreso che dell'amministratore abbiamo ancora bisogno, ora togliamolo di mezzo, liberiamocene definitivamente e così vengo alla domanda sulla necessità di fidarsi del gestore del sito.

Prof. Vincenzo Rana: Aggiungo solo una cosa velocissima. Stiamo parlando del fatto che la banca non può fare transazioni a mio nome perché sono firmate, ma ora vi faccio vedere un'altra cosa interessante. Ipotizziamo che oggi mi voglia collegare alla banca per fare un bonifico, però se il sito non è raggiungibile per qualunque motivo il bonifico non posso farlo, devo aspettare domani; quindi, mettiamo che io volessi pagare Francesco ma il sito non sta andando, non è disponibile o la banca non funziona o mi blocca il conto:

io quei soldi non li posso in nessun modo trasferire. Invece nella modalità che stiamo spiegando posso prendere il mittente, inserire il mio *address* quindi la mia identità, come destinatario metto Francesco, inserisco la quantità, firmo correttamente.

Prof. francesco Bruschi: Sì sì, questo è vero, è il prossimo passo. Qui siamo ancora al punto in cui gli utenti mandano le loro transazioni, ma ci deve essere un amministratore che fa solo quello: le colleziona e le pubblica. Se quando voglio fare un pagamento lo mando all'amministratore, l'amministratore lo riceve e lo pubblica. Attenzione, quindi abbiamo compresso l'amministratore, ma serve ancora: in particolare qui ha proprio il compito di ricevere le transazioni e magari tra l'altro gli arrivano delle transazioni che sono state generate contemporaneamente. Magari io e Vincenzo mandiamo contemporaneamente un mandato di pagamento e ovviamente è cruciale che questi mandati, queste transazioni, vengano eseguite in un ordine preciso. Chi decide questo ordine? Lo decide l'amministratore che ha ancora delle prerogative, seppure ridimensionate, comunque significative. Altra prerogativa dell'amministratore è la censura, cioè se l'amministratore decide che io, controllore di questa chiave pubblica che ho 10 *voucher*, devo essere bloccato o vuole congelarmi il conto lo può fare. In che modo? Semplicemente quando io gli manderò le transazioni, lui non le includerà mai in questa lista. Può dire che non le ha ricevute. Insomma, ha ancora il potere di censurare gli utenti, quindi di congelarne i conti e ha un altro grande potere: spegnere tutto il sistema. Quindi, come diceva Vincenzo, se ad un certo punto, per qualsiasi ragione, l'amministratore non è disponibile perché subisce un attacco, perché lui stesso vuole portare un attacco al sistema, il sistema si blocca. Quindi, abbiamo compresso l'amministratore ma ne abbiamo ancora bisogno.

Vorremmo allora liberarci dell'amministratore ed ecco che arriva la seconda grande innovazione: il contributo di questo misterioso *Satoshi Nakamoto*, di cui immagino abbiate sentito parlare. Uno pseudonimo che copre la vera identità del soggetto. Se sia un individuo o molti, uomo o donna, non lo sappiamo. Nel 2008 questo personaggio pubblica un articolo ormai storico, nel quale propone un sistema di elaborazione che decentralizza il compito dell'amministratore: dove prima ci serviva un amministratore, adesso *Satoshi Nakamoto* propone una rete dinamica di soggetti che eseguono il compito dell'amministratore in modo trasparente, cioè tutti possono verificare effettivamente che le regole dell'amministrazione siano applicate, che le firme siano verificate, che il soggetto che spende i soldi li abbia veramente. Non è possibile per nessun soggetto interno o esterno bloccare questo sistema, cioè arrestare la pubblicazione di queste transazioni mandate dagli utenti e l'ag-

giornamento della tabella dei conti, che non è censurabile né da attori interni né da attori esterni al sistema, essendo impossibile impedire a un attore di trasferire e di inviare un suo assegno e quindi vedere trasferiti i suoi *voucher*. Potremmo, per i nostri scopi, accontentarci di questo. Potreste credere a me che effettivamente l'articolo *Satoshi* propone un sistema di questo tipo che funziona.

Ecco, vi vorrei dare qualche idea su come funziona, come è possibile prendere il compito dell'amministratore e trasferirlo su una moltitudine di soggetti. Attenzione, moltitudine di soggetti che è dinamica: cioè non è che io prendo l'amministratore e lo sostituisco con 10 amministratori, cosa che comunque renderebbe il sistema meno soggetto all'arbitrio di un singolo amministratore. No, io qui sostituisco l'amministratore con un insieme dinamico di soggetti a cui chiunque può partecipare. Cioè, oggi, se volessimo fare una piccola parte del lavoro dell'amministratore, potremmo farlo. Chiunque di noi potrebbe farlo con mezzi tecnici tutto sommato accessibili. E allora com'è possibile che succeda questo? Anche tenuto conto del fatto che l'amministratore, in questo caso, può essere chiunque, non possiamo più fidarci del fatto che lo stesso sia affidabile, che sia orientato a comportarsi secondo le regole. È un'affermazione che non possiamo più fare, che cade. Come fa il sistema a spingere tutta questa miriade di amministratori a comportarsi correttamente? Attraverso la trasparenza dell'esecuzione e un meccanismo di incentivazione economica. Questo è uno dei punti più innovativi, interessanti, potremmo parlarne per ore. Lasciatemi provare a dare un'idea.

Avete sicuramente sentito parlare del *Mining* e del *Proof of Work*, che si è guadagnato un po' di titoli di giornali. Che cos'è il *mining*? In questo sistema è un meccanismo che consente di incentivare/disincentivare economicamente questi attori che vogliono concorrere a fare il lavoro dell'amministratore. La logica è questa: se io mi voglio candidare a fare il l'amministratore, concretamente che cosa vuol dire? Vuol dire che farò il lavoro di scegliere e pubblicare un certo numero di transazioni degli utenti nel prossimo futuro. Se adesso voglio farlo il sistema mi dice "*guarda, tu devi fare così: scegli le transazioni, gli assegni che vengono pubblicati nei prossimi 10 minuti. A questo punto, date queste transazioni, ti chiedo di risolvere un problema matematico molto costoso computazionalmente che tu puoi risolvere al prezzo di far funzionare un computer e spendere molto in energia elettrica. Questo problema una volta che tu l'hai risolto ce ne dai la prova e chiunque può verificare effettivamente che tu l'abbia risolto e, cosa fondamentale, che tu abbia effettivamente speso una certa quantità di energia per fare questa cosa (1 kw ora, 10, 100 kilowatt ora, ecc.) e che quindi tu hai speso delle risor*se". Spendendole sei

finito in una situazione di soggezione economica, quindi sei in perdita. Questo è importante perché a questo punto il sistema se mi comporto bene – se quindi faccio il mio lavoro correttamente e aderisco alle regole – mi dà una ricompensa. In che modo? Sotto che forma? Beh, il nostro amministratore che cosa ha a disposizione? Può creare dei *voucher*, quei *voucher* che volevamo contabilizzare possono essere creati dall'amministratore, che quindi nella riga della mia tabella può, perché le regole lo consentono, darmi un premio. Mi metto in soggezione economica, facendo *mining*, spendendo energia, ma se poi faccio il bravo riceverò un premio, se non faccio il bravo non riceverò quel premio e quindi sostanzialmente sarò stato punito. Ed ecco qua l'idea dirompente, se volete, geniale, di *Satoshi*. Quando venne presentata questa idea, mi ricordo di averla letta poco dopo. Era proprio il 2008/2009. È un'idea bizzarra, è un esperimento estremamente fantasioso. Perché un soggetto dovrebbe volere fare *mining*, dovrebbe voler fare il validatore? Perché riceveva questo premio. Ma questo premio in cosa consiste? Consiste in questi *voucher* che sono contabilizzati all'interno del sistema. Che valore hanno questi *voucher* e perché dovrebbero avere un valore? All'inizio questa cosa non era evidente ma se andiamo avanti veloce fino ad oggi, invece, vediamo che oggi questi *voucher* sono poi i *Bitcoin* e uno di questi oggetti oggi vale svariate decine di migliaia di dollari.

Ho provato a darvi un'idea molto veloce di che cosa sia il mining, ovviamente rappresentata in modo semplificato. Spero però di avervi dato qualche elemento.

Dott. Fabio Di Vizio: si stava profilando qualche domanda, ma chiedo un po' di pazienza e di porla a chiusura dell'intervento, consentendo una continuità di esposizione, perché alcuni presupposti tecnologici vanno illustrati in continuità lungo la loro evoluzione.

Prof. francesco Bruschi: Sì, d'accordo, assolutamente. Allora quello che abbiamo ottenuto è il *Bitcoin*. Il nostro famoso *Bitcoin* è questo: un sistema di contabilizzazione di *asset* digitali, la nostra prima criptovaluta. Gli utenti possono partecipare tramite quell'identità che abbiamo visto, che può essere generabile in maniera autonoma, che non può essere interrotta da nessuno né dall'interno né dall'esterno e non può essere censurata.

L'altro aspetto importante è la cosiddetta politica monetaria, ovvero: quanti *Bitcoin* ci sono? Chi lo decide? Questo è determinato dal protocollo dell'amministratore che stabilisce chiaramente quanti *Bitcoin* possono esserci, vengono generati e quanti ne esisteranno mai. In particolare oggi i validatori vengono ricompensati con un certo numero di *Bitcoin*. Questa quantità si dimezza periodicamente e si dimezzerà fino ad arrivare a zero e a quel punto

saranno stati creati dall'inizio del sistema 21 milioni di *Bitcoin* e nessun altro *Bitcoin* potrà essere creato. Quindi questo è un altro prodotto collaterale di questa idea: abbiamo creato degli oggetti digitali scarsi, ce ne sono 21 milioni, ma è una quantità definita e deterministica. Sappiamo che *Bitcoin* parte come un esperimento creato da appassionati di informatica, pian piano però arrivano utenti, attori e questi oggetti cominciano ad apprezzarsi, si creano mercati sui quali vengono scambiati e, come sappiamo, oggi valgono decine di migliaia di dollari, quindi di euro. Nel 2010 c'è stato il primo pagamento documentato in *Bitcoin*: sono state acquistate due pizze, non sappiamo che tipo di pizza, ma sono stati pagati 10.000 *Bitcoin*. Oggi il *Bitcoin* viaggia fra i 30.000 e 50.000 $: fate un po' due conti su quanto sono state pagate quelle pizze al valore attuale del *Bitcoin*.

Dott. Fabio Di Vizio: Una breve osservazione su questo argomento. Lei ha introdotto il tema del trasferimento dell'informazione e del trasferimento del valore. Fondamentalmente, questa è la traccia che stiamo cercando di ripercorrere. Andando sul sito *CoinMarketCap.com*, avete la possibilità di vedere qual è la capitalizzazione orientativa del settore: stiamo parlando di circa 1280 miliardi di dollari. Attualmente il *Bitcoin* vale un po' meno di quello che si accennava, siamo attorno a 28.000 $, è una fase flettente, ma stiamo parlando comunque di qualche cosa che rispetto ad anni fa ha acquisito dimensioni che vanno tenute in considerazione. In questo calderone ci sono naturalmente interessi che esamineremo nella parte successiva, ma ci sono anche gli interessi di qualsiasi risparmiatore che cerca un'occasione di proficuo investimento in un momento storico nel quale altre prospettive sono meno appetibili.

Prof. francesco Bruschi: Assolutamente. Quindi, *Bitcoin* introduce questo meccanismo. Qualche anno dopo, nel 2013 a qualcuno viene in mente questa possibile generalizzazione: stiamo parlando di *blockchain*, ossia la sequenza di transazioni che vengono compilate in maniera crescente nel tempo. Questo è la *blockchain*, la sequenza delle transazioni che gli utenti hanno inviato al sistema, quella struttura dati che contiene tutta l'informazione che serve per capire lo stato attuale, la contabilità attuale. Qualcuno dirà: "*Ma perché invece di eseguire soltanto quel semplice programma, quello che rappresenta l'amministratore del Bitcoin, non creiamo una piattaforma in cui si possono eseguire logiche arbitrarie con quelle interessanti caratteristiche che ha l'amministratore di Bitcoin, cioè trasparente e non interrompibile e non censurabile?*" È da questa idea che nel 2013 diverse persone, tra cui *Vitalik Buterin*, hanno avuto l'idea di una piattaforma che possa eseguire qualsiasi programma: sono gli "*Smart contract*" e ci sarebbe tantissimo da dire

se questi siano dei contratti e se siano *smart*. Questa piattaforma viene ideata e apre una serie di possibilità applicative che vado a raccontarvi. Oggi con *blockchain* non si intende tipicamente solo la struttura dati propriamente che abbiamo visto, ma una piattaforma che, in virtù anche di quella struttura dati, è in grado di eseguire programmi con le caratteristiche che dicevamo. Cosa ce ne facciamo? Nel 2013 nasce *Ethereum*, che è a tutt'oggi la principale piattaforma per esecuzioni degli *smart contract*. Che cosa ce ne facciamo di questa possibilità generalizzata? Se il trasferimento di *asset* digitali era quello che già si poteva fare con *Bitcoin*, cos'altro possiamo fare? Prima facevo l'esempio della cooperativa di *baby sitter* che vuole creare dei *voucher* da scambiarsi. Ebbene, a questa esigenza non risponde *Bitcoin*, le famiglie non si scambiano *Bitcoin* ma vorrebbero creare una serie di *voucher* in quantità limitata che poi servono per lo scambio interno. Ebbene, questa cosa su *Ethereum* la possiamo fare, quindi possiamo definire degli *asset* generici con proprietà programmabili arbitrarie che vengono chiamati *token*. Che cosa ce ne facciamo di questi *token*? Si possono fare moltissime cose. Una delle applicazioni più attuali è quella della rappresentazione del valore. Che cosa voglio dire? I *Bitcoin* hanno oggi un valore estremamente volatile e sarebbero poco pratici se volessimo utilizzarli per pagare il caffè. Pago il caffè al bar dando ovviamente non un *Bitcoin*, ma una frazione, un millesimo di *Bitcoin*. Cosa succede? Che il barista riceve in *Bitcoin* il valore di 1 € oggi, ma domani quanto varranno? Non lo sappiamo, perché è volatile: allora è possibile creare all'interno di una piattaforma come *Ethereum* dei *token*, che con alcune tecniche possono essere stabilizzati. Il loro valore può essere indotto e agganciato a quello di un asset esterno, come per esempio il dollaro o l'euro. E qua abbiamo tanti strumenti tra cui il famoso *Terra*, di cui avrete sentito parlare, collassato proprio la settimana scorsa in una delle più drammatiche capitolazioni di una parte del mondo delle criptovalute.

Dott. Fabio Di Vizio: Siccome è una vicenda d'attualità, credo che sarebbe utile che il prof. Bruschi volesse offrire qualche indicazione su che cosa possa rendere possibili queste "capitolazioni". Le *stablecoin*, infatti, sono quanto di più si avvicina alla funzione monetaria socialmente riconosciuta, almeno secondo i canoni classici, e questo aiuta a comprendere la necessità di governare i funzionamenti, anche creativi, di questa tecnologia.

Prof. francesco Bruschi: Dico subito qual è un modo semplice concettualmente, per creare un oggetto che abbia il valore di 1 $. Attraverso queste piattaforme io posso costituire una società che tecnicamente può creare dei *token* di un certo tipo, cioè oggetti attraverso una tabella come quella che abbiamo visto prima. Questa tabella non è quella di *Bitcoin*, ma di un *token*.

Questo *token* a questo punto sarà scambiabile tra soggetti, esattamente con quelle interessanti modalità delle quali dicevamo prima. Ora se volessi creare un insieme di *token* (siano 10, 100 oppure 1000) che hanno il valore di 1 $, utilizzabili per esempio nell'economia, per pagare il caffè, potrei dire: "*Cari utenti, io faccio questo lavoro, ho creato 100 token, 1000 token, ora voi potete venire da me a darmi 1 $, io prendo il dollaro, lo metto in una cassaforte e vi trasferisco uno di questi token, poi voi lo trasferite a chi volete*". A questo punto ci sarà un *token* in circolazione. Se qualcuno mi restituisce questo *token* io mi impegno ad andare alla cassaforte e ridargli il dollaro. Ovviamente poi lo faccio per 1 dollaro, per 100, per mille, e metterò in circolazione dei *token* che i soggetti si scambieranno come se fossero 1 $ ciascuno, perché convinti in ogni momento di potere venire a riscuoterli da me.

Dott. Fabio Di Vizio: È la forma moderna della vecchia parità aurea?

Prof. francesco Bruschi: Esattamente. Qui noterete subito che abbiamo reintrodotto una centralizzazione riferibile al soggetto che custodisce questi dollari: però, se questo soggetto si comporta onestamente, il sistema funziona. Funziona perché questi *token* hanno un controvalore effettivamente in un bene che ha un valore costituito dai dollari "ricoverati" in cassaforte, o dall'oro, nel caso dello standard aureo. Attenzione, Terra non faceva esattamente così, faceva una cosa più fantasiosa: emetteva *stablecoin*, ma non richiedeva un controvalore in dollari veri, in oro, in garanzie tramite immobili, ma emetteva un altro *token* che avrebbe dato diritto, per chi lo possedeva, di percepire alcune commissioni sullo scambio dello *stablecoin*. È una prospettiva, in qualche modo, autoreferenziale: cioè io ti do una cosa che dico vale 1 $ che è garantita da un diritto sulle commissioni sullo scambio di questi dollari nel futuro. Allora questo è un sistema che funziona se tutti sono convinti che il sistema funzioni; in questo senso dico che ha componenti di autoreferenzialità.

Dott. Fabio Di Vizio: Quindi il collaterale era un po' rischioso?

Prof. francesco Bruschi: Il collaterale era rischioso ma non solo: era collegato allo *stablecoin* e quindi i due erano avviluppati in un intreccio fatale, perché nel momento in cui qualcuno comincia ad avere dei dubbi sul valore dello *stablecoin* automaticamente ha dubbi anche sul collaterale perché il valore del collaterale dipende dal valore dello *stablecoin*, secondo un circolo vizioso. Però questo incantesimo ha funzionato per diverso tempo, per almeno un paio d'anni. Poi il valore di questo sistema è cresciuto fino ad arrivare a 50, 60 miliardi di dollari di valore fino alla settimana scorsa, in cui in tre giorni è stato oggetto di un attacco sicuramente molto abilmente programmato, con cui è stato manipolato per un po' di tempo il valore dello *stablecoin*.

Questo normalmente può succedere ma è una cosa che viene assorbita se il valore dello *stablecoin* è garantito da del valore; in questo caso il meccanismo di garanzia era questo *loop* senza fondamento e tutto è crollato nel giro di tre giorni, tra l'altro con conseguenze drammatiche: alcuni investitori hanno perso moltissimo.

Questo è uno dei possibili *stablecoin*, ma ce ne sono altri: per esempio quelli semplici collateralizzati di cui abbiamo detto, e ci sono versioni anche decentralizzate ma assolutamente collateralizzate, in cui c'è una garanzia rispetto a questi *token*, ma la garanzia non è gestita da un attore o da una società che possa scappare con i "soldi", ma è gestita da un amministratore sulla *blockchain* completamente trasparente e quindi senza rischi di controparte.

Dott. Fabio Di Vizio: Professore, mi interessava adesso cominciare ad affrontare il tema dei "nuovi" intermediari. In altri termini, in un mondo costruito sull'idea della totale e "magnifica" disintermediazione, in apparente controtendenza, abbiamo costante l'esperienza di siti o comunque di ambienti che danno ingresso più direttamente al mondo della *blockchain* attraverso tipici meccanismi di intermediazione.

Prof. francesco Bruschi: Certo. Lasciatemi concludere questa parte sulle *blockchain* dicendo che le stesse introducono una piattaforma che, in modo innovativo, consente di eseguire programmi in modo affidabile. Normalmente quando ci colleghiamo al sito dobbiamo fidarci di chi lo gestisce. Qui non devo fidarmi che quel soggetto esegua correttamente e non manipoli, per esempio, il codice che è in esecuzione, poiché questo viene garantita dalla piattaforma. Ciò apre a tante possibilità. Potremmo citare molto velocemente possibili applicazioni, tra cui assicurazioni decentralizzate, oppure prestiti collateralizzati. Nel campo della pubblica amministrazione, per esempio, si potrebbero fare gare d'appalto garantite a priori, votazioni, graduatorie e tutta una serie di cose estremamente interessanti.

Sviluppando questo ragionamento, immaginiamo di voler "giocare" con questi strumenti. Immagino di voler entrare anch'io in questo sistema e volere, per esempio, farmi trasferire alcuni di questi *Bitcoin* perché poi li voglio usare o tenerli, sperando che il prezzo salga, oppure per farci qualcosa, per pagare, perché finalmente hanno un valore; in concreto tutto ciò che ha valore ed è trasferibile lo posso usare come forma di pagamento. Come faccio? Quello che vedremo fra poco è uno strumento che ci serve, che possiamo utilizzare: quello dei *Wallet*, che consentono di fare quello che dicevo prima, cioè generare le chiavi pubbliche e private, collegarci alla *blockchain*, firmare transazioni in modo del tutto autonomo e in questo modo posso creare un'identità. Ora voglio anche entrare in possesso di alcuni di questi *Bitcoin*,

voglio comprarli. Come faccio? Arriviamo alla questione assolutamente centrale.

Oggi se voglio comprare dei *Bitcoin* o degli *Ether* (che sono la valuta di *Ethereum*, la principale piattaforma di esecuzione di *smart contract*) o qualsiasi altra criptovaluta, ho diversi modi per farlo. Un modo di gran lunga più accessibile a chiunque è quello di utilizzare un *Exchange*; qua ho messo in evidenza "centralizzato". Che cos'è un *Exchange* centralizzato? È un soggetto che possiede criptovalute, con quelle modalità che dicevamo prima, che è disposto a vendere; sono soggetti controllati da società, per la maggior parte regolamentati e hanno un sito. Per esempio – vado sul sito – se i soggetti sono, per esempio *Coinbase*, *Kraken*, mi registro con le solite modalità tipiche e a questo punto posso pagare con bonifico bancario, con carta di credito e posso comprare questi *token* pagandoli con i meccanismi di pagamento consueti. Questa è una funzione fondamentale che svolgono questi attori, che viene chiamata normalmente di *on ramp*, cioè di ingresso al sistema. Attenzione: gli Exchange non si limitano a questo ma tipicamente mi danno accesso ad un'altra possibilità fondamentale. Per quello che ho detto prima il possesso di questi asset lo posso controllare direttamente senza chiedere niente a nessuno, attraverso quel meccanismo di chiave pubblica - chiave privata. Si tratta di un meccanismo sicuramente affascinante, però ha problematiche: per esempio cosa succede se perdo la chiave privata?

Dott. Fabio Di Vizio: Vorrei rimarcarlo questo concetto. L'esistenza degli *Exchange* centralizzati offre anche opportunità in termini investigativi, perché, come adesso verrà meglio spiegato, la custodia delle chiavi, anche quelle private, in controtendenza rispetto ai postulati di questa tecnologia, non è più nelle disponibilità degli *users*, cioè di coloro che hanno aperto il conto, ma dello stesso gestore della piattaforma. Vedete, questo cambia concretamente lo schema astratto, orientato verso un'altra soluzione; ciò offre opportunità investigative, ma espone anche a rischi. È un tema sul quale dopo mi tratterrò più a lungo, nella sessione dedicata alla qualificazione giuridica di una serie di condotte.

Prof. francesco Bruschi: Rimarco anch'io questo aspetto. Una volta che vado su *Coinbase* o su *Binance*, apro una posizione, mi registro; questi attori, tipicamente, sono soggetti agli obblighi di identificazione e quindi mi identifico tramite documento d'identità. A questo punto ho aperto un *account* presso questo *Exchange*. Compro dei *Bitcoin*, e li pago con la carta di credito. Questi *Bitcoin* a chi vengono trasferiti in quella famosa tabella che avevamo prima, a una riga che è controllata da una chiave che controllo personalmente? Molto più spesso quello che succede realmente è che l'*Exchange* mi dice

"*guarda, non ti preoccupare tu di tenere le chiavi, è pericoloso, non fa per te, i Bitcoin che hai comprato te li custodisco io*". Che cosa vuol dire te li custodisco io? Vuol dire che crittograficamente sono nel controllo della piattaforma, quindi io non conosco la chiave privata; il titolo che ho è il riconoscimento da parte di *Coinbase* del fatto che io sono proprietario di uno o due o 0,5 *bitcoin*. Questa modalità di custodia viene chiamata *Custodial* o *Hosted Wallet*. Che cosa succede se io voglio trasferire dei miei *token* a qualcun altro? Ho due modalità: o li posso trasferire alla chiave pubblica che controlla direttamente l'altra persona, oppure quest'ultima, esattamente come me, ha anche lei ha un *account* su *Coinbase*; in questo caso do mandato a *Coinbase* di cambiare la sua contabilità interna e di rappresentare che adesso io ho 0,1 *Bitcoin* in meno e l'altro utente invece ne ha di più.

Dott. Fabio Di Vizio: In *blockchain* cosa va? Nel caso che rappresentava, in cui Lei si trova in piattaforma dell'*Exchange* e anch'io ho un *address* sulla stessa piattaforma, cosa va in *blockchain*, in caso di trasferimento registrato dalla contabilità interna della piattaforma?

Prof. francesco Bruschi: Sulla *blockchain* non va niente, cioè se uno guarda quel registro di transazioni non vede niente, non c'è stato un trasferimento. Perché la disponibilità dei *Bitcoin* crittograficamente è ancora tutta in carico a *Coinbase* che ha aggiornato la sua contabilità interna esattamente come una Banca commerciale, come se facessi un bonifico all'interno della Banca commerciale: non si muove niente, si muove soltanto la contabilità interna.

Dott. Fabio Di Vizio: Quando tornerà in *blockchain*?

Prof. francesco Bruschi: Quando il soggetto titolare della posizione su *Coinbase* chiede a quest'ultimo: "*Guarda che tu mi stai custodendo due* Bitcoin*. Ora ti chiedo di trasferirli invece a questo altro* address *crittografico*", che magari controllo. A questo punto che cosa fa *Coinbase*? Prende due dei suoi *Bitcoin* che controlla, che ha nella sua riserva e li trasferisce, questa volta in *blockchain*, a un indirizzo, quindi ad una chiave pubblica che è esterna. A questo punto *Coinbase* non ha più un controllo di quegli *asset*. Quindi io posso sempre entrare in possesso e controllare i *token*, secondo le modalità molto forti che dicevamo. Quello che succede è che molto spesso gli utenti non lo fanno, quindi sostanzialmente tengono dei conti in *Bitcoin*, ma con modalità tecniche del tutto affini a quelle dei conti bancari, salvo la possibilità di uscire.

Un'altra cosa che si può fare con gli *Exchange*, da qui il nome, è scambiare *asset* di tipo diverso. Come dicevo prima, queste piattaforme consentono di definire e di creare degli asset che rappresentano cose diverse. Qui

non soltanto *Ether* o *Bitcoin*, ma anche i *voucher* del *baby-sitter* nel nostro esempio, ma anche buoni che rappresentano diritti a flussi di ricavi futuri di società, più un sacco di altre cose che possono avere un valore e che possono essere scambiate. Quindi posso "giocare": esattamente come scambio le azioni di *Apple* con quelle di *Amazon* posso giocare a scambiare un *token* con un altro. Questa cosa, *l'Exchange* mi consente di farla sempre con quelle modalità. Quindi *Exchange* tiene il controllo di questi *token* e aggiorna la propria contabilità interna. Questo ovviamente espone a rischi sostanzialmente di due tipi: anzitutto a rischi di controparte. Se guardiamo la storia di queste tecnologie, la maggior parte dei problemi sono dovuti a debolezze degli *Exchange* centralizzati che non sono adeguati e vengono "bucati", cioè compromessi, oppure sono malevoli. Ovviamente, come giustamente si evidenziava, qui stiamo tornando al mondo "vecchio", in cui l'onestà e la capacità degli intermediari è fondamentale perché altrimenti richiamo di perdere i nostri soldi. Perciò si è sviluppato, e si stanno sviluppando alternative decentralizzate, soprattutto su *Ethereum*. Queste alternative sono le piattaforme in cui c'è un amministratore che gira nelle modalità che dicevamo, quindi del *software* garantito dalla tecnologia alla sua esecuzione, che consente agli utenti di scambiarsi i *token* senza però quei rischi di controparte che dicevamo. Quindi non mi fido di una persona, ma della correttezza del codice, posto che è pubblico, che posso ispezionare e verificare.

Questo pone un'altra questione che immagino sia rilevante per voi. Che cosa succede se a un certo punto un'autorità vuole imporre qualche cosa a un *Exchange*? Questo è successo veramente nel caso di *Uniswap*, che è il principale *Exchange* decentralizzato: la SEC ha squalificato alcuni di questi *token*. Insomma, ha imposto a *Uniswap* di eliminare questi *token*. Ma *Uniswap* chi è? Lo *smart-contract* che gestisce questo *Exchange* non è controllabile da nessuno, non c'è nessun soggetto, nessuna società che possa fare questo, quindi effettivamente c'è stato un *delisting*, ma è stato un *delisting* dall'interfaccia. Infatti, a questi *smart contract* tipicamente si accede attraverso un'interfaccia classica *web* e quell'interfaccia può essere modificata in modo da inibire, per esempio nel caso di *Uniswap*, il trasferimento, la negoziazione di certi *token*. Attenzione, questo è possibile farlo, ma l'interfaccia può essere con grandissima facilità bypassata; quindi, è facilissimo creare un'altra interfaccia riabilitando lo scambio.

Concludo con un tema che poi svilupperemo dopo, che è quello della tracciabilità. Si potrebbe pensare: "*Ma qui questi sistemi effettivamente consentono di operare finanziariamente in maniera anonima, nel bene e nel male?*". La risposta è: sì e no. Noi abbiamo detto che gli utenti sono pseudo-

nimi, quindi chiunque può autonomamente creare un'identità senza chiedere niente a nessuno e immediatamente diventare un attore economico attivo, facendosi trasferire degli *asset* e a sua volta poi trasferendoli. Quindi questo nessuno può impedirlo, né può premettergli l'obbligo di identificazione. Questo sembrerebbe andare nella direzione della *privacy* e dell'opacità. Però attenzione. L'altra cosa che dovremmo aver capito è che tutte le transazioni sono visibili pubblicamente. Dunque, è vero che io posso creare identità in quattro e quattr'otto e poi farmi trasferire degli asset, però questo trasferimento è pubblico e può essere visto da chiunque. Si possono fare delle analisi induttive per sapere di chi è l'indirizzo X, andare a vedere chi lì ha trasferito *asset* e poi, a sua volta, chi è questo e da chi ha ricevuto gli asset e così via, fino ad arrivare a qualche punto noto, perché magari a un certo punto si arriva a un trasferimento in uscita da uno degli *Exchange* centralizzati di cui parlavamo prima. A quel punto ho un'identità, perché vado dall'operatore e posso chiedergli chi c'è dietro quel trasferimento e posso fare dei ragionamenti induttivi che mi possono portare poi anche all'identificazione di soggetti che sarebbero invece nativamente scollegati e non identificabili. Questa è una cosa che non è solo teorica, la si fa sempre più spesso e sta portando sempre più risultati, tant'è che in realtà il luogo comune secondo cui *Bitcoin* sono lo strumento ideale per attività illecite, vacilla proprio per il successo di alcune azioni investigative che portano con successo a individuare i responsabili di azioni criminose o penalmente rilevanti: quindi la tracciabilità esiste.

Ma voglio concludere con una nota al contrario: trovato il modo di fare una cosa, ovviamente, sono stati sviluppati degli strumenti che invece consentono di far perdere di nuovo le tracce. Uno sicuramente dei più diffusi è quello dei *mixer* che dopo, se riusciamo, vedremo in funzione. Concretamente, come funziona un *mixer*? In un *mixer* sostanzialmente posso conferire degli *asset* a una piattaforma e poi conferisco un cosiddetto *commitment* che è un numero che deriva da un segreto che conosco, e poi è possibile fare il giro e ripresentarsi al negozio con una prova crittografica che dimostra il mio diritto di riscuotere uno dei sacchetti presenti nel negozio ma in modo che questa riscossione non possa in nessun modo essere associata in modo logico a un particolare deposito. Quindi con i *mixer* sostanzialmente possiamo andare a interrompere quelle catene di tracciabilità di cui dicevo prima. Ecco giusto una precisazione: uno strumento così uno lo guarda e dice: "*Questo ovviamente nasce con intenti e finalità esclusivamente criminali, chi potrebbe fare una cosa del genere?*". Consideriamo, invece, che in questo mondo, in questo sistema, tutto è in piazza; quindi, anche se qualcuno volesse utilizzarlo come sistema di pagamento, immagino un barista che accetta pagamenti in *Bitcoin*,

si troverebbe con tutti i conti esposti pubblicamente: io vado, pago il caffè, sto al suo indirizzo, posso "farmi i fatti suoi".

Dott. Fabio Di Vizio: Infatti alcuni Paesi immaginano una moneta pubblica che dovrebbe essere utilizzata e che dovrebbe rendere del tutto tracciabile e per sempre ogni movimento. Questo offre uno scorcio su aspetti particolari: una tecnologia implementatasi nella ricerca di una riserva esclusiva del controllo della risorsa, per togliere o limitare il controllo di un intermediario, di un'autorità pubblica o anche privata, giunge ad assicurare una tracciabilità pubblica, senza segreto e senza oblio. In effetti, un esito interessante e forse inatteso. Infatti, alcuni Paesi – la Cina è uno di quelli su cui stiamo svolgendo le analisi più approfondite – immaginano di adottare la valuta virtuale di Stato come strumento che rende tutto assolutamente trasparente e controllabile dall'autorità pubblica; perché poi il controllo, come lo può fare il privato, lo può fare, naturalmente, anche l'autorità pubblica. In generale, va considerato che a nuove opportunità corrispondono nuove implicazioni. Per questo in apertura vi invitavo a tener conto di implicazioni che possono andare in direzioni in parte impreviste. Ora non so se ha finito, professore?

Prof. Francesco Bruschi: Volevo solo aggiungere un'osservazione alla sua ultima considerazione. Lei parla di quelli che tecnicamente si chiamano CBDC, *Central Bank Digital Currencies*, cioè *token* sostanzialmente del tipo di cui abbiamo parlato, che vengono emessi non da un soggetto privato ma da una Banca centrale, per rappresentare in modo digitale il denaro con tutti i vantaggi che abbiamo visto. In questo progetto davanti a tutti c'è la Cina, che ha già sperimentato ampiamente alcune forme di moneta digitale di questo tipo e ovviamente in Cina possiamo pensare che i requisiti di *privacy* possano essere percepiti in maniera diversa. È interessante notare come tutte le maggiori Banche Centrali mondiali si stanno attrezzando per provare a realizzare delle forme di denaro digitale e tra queste c'è sicuramente anche la BCE. Qui uno dei punti che sono emersi da alcuni sondaggi che sono stati fatti è che invece la *privacy* è un punto forte. Quindi tu, Banca, mi dai *token* che hanno l'ambizione di sostituire il denaro contante, però mi devi garantire che non puoi spiare quando vado a prendere il caffè e quindi sarà necessario tenere queste cose in considerazione. Non so se poi il meccanismo saranno i *mixer*, ma qualche meccanismo per garantire la privacy dei cittadini dovrà essere considerato.

Dott. Fabio Di Vizio: Lei invita ad un atteggiamento più pragmatico anche sul *mixing* quale tecnica difensiva rispetto ad alcune esigenze commendevoli. D'altro canto ricordo come le fiduciarie, nel nostro ordinamento, abbiano ricevuto una disciplina organica con una legge del 1939; un testo nor-

mativo nato in una temperie storica nella quale le fiduciarie servirono anche a proteggere rispetto a condotte espropriative nei confronti di appartenenti alla comunità ebraica, assicurando il presidio di alcune loro risorse. Anche questo per dirvi come, dinanzi ad un fenomeno così multiforme, dobbiamo abituarci a esaminarne ogni caratteristica senza preconcetti; è l'aspetto e la proposta, anche sfidante, che ho ritenuto di proporvi.

A monte, in ogni caso, non possiamo impostare nessuna analisi giuridica né investigativa se non conosciamo davvero il funzionamento del fenomeno. Gli ingegneri del Politecnico studiano e cercano di implementare le potenzialità positive, tecnologicamente avanzate e socialmente utili delle valute virtuali. Come pubblici ministeri e inquirenti cerchiamo di esaminarne il funzionamento, per capire come possono divenire strumenti di alcuni meccanismi criminali, di occultamento e di reimpiego. Usualmente, invece, nella spiegazione della realtà fenomenica delle criptovalute, si passa subito alle classificazioni, alle definizioni, dando per scontato che tutti conoscano a fondo il loro funzionamento.

Vi racconto un'esperienza personale: non entrerò nel tema di dettaglio, ma circa due anni fa un *Exchange* che si occupava di cambio di valute virtuali in altre valute virtuali non è stato più in grado di restituire le risorse che aveva e che contabilmente imputava ai diversi clienti. Inizialmente mi domandavo come fosse possibile, a fronte di una tecnologia orientata ad assicurare il controllo immediato ed esclusivo della risorsa, che invece questi soggetti, gli *users* nel linguaggio di settore, non fossero più nelle condizioni di ritirare quello che, come saldo, risultava in corrispondenza del loro conto, per usare adesso un'immagine evocativa di schemi classici conosciuti nei rapporti con gli intermediari bancari. Andando ad approfondire la tematica, ho compreso che la concreta gestione di tali risorse era centralizzata; le risorse venivano fatte passare da *address* individuali, ma a loro volta poi venivano svuotati, peraltro secondo operatività non originale, perché questo, piuttosto, è il funzionamento ordinario della più parte di tali piattaforme.

Questa è una cosa di cui è opportuno che si tenga conto perché consente di cogliere il concetto che evocavo quando accennavo a nuove opportunità: sapendo come funziona la piattaforma si può sapere come e cosa cercare. A fronte dell'ammanco, cioè di un deflusso realizzato perché lo stesso cliente prelevava più volte e il sistema non registrava i primi prelievi – al pari di un saldo bancario permanentemente invariabile al quale si attinga senza fine in difetto di annotazione dell'operazione di prelievo precedente – l'amministratore della piattaforma non è più stato nelle condizioni di restituire le risorse. Alcuni clienti della piattaforma e il pubblico ministero hanno dovuto avanza-

re una richiesta di fallimento del soggetto impossibilitato a restituire le risorse immagazzinate. Ma di chi erano quelle risorse, chi le controllava? Questo è il problema più impellente che si è posto in questa fase e spiega anche il modo con il quale il diritto tradizionale si avvicina a questa materia.

L'inquadramento giuridico, qui, è sempre complesso, la tecnologia ha profili di originalità assoluti. Il professor Bruschi ha ben spiegato come si sia in presenza di intuizioni originali, geniali, ma la novità è sempre una sfida ed un impegno per il diritto. E noi abbiamo categorie giuridiche antiche che talvolta sono elastiche, ovvero in grado di ricomprendere un fenomeno, talvolta lo sono meno e non ci riescono. Pensate, poi, quanto questa problematica possa amplificarsi nel diritto penale. Lo *jus terribile*, infatti, per non essere troppo terribile, è retto da rigorose regole di legalità e di tassatività nella definizione di un precetto; quale interprete devo immaginare che un precetto – si pensi all'abusivismo finanziario piuttosto che a quello di investimento – emanato quando ancora non c'erano queste nuove tecnologie e queste nuove risorse, sia comunque in grado di governarle. Si pensi al trattamento tributario, di contabilizzazione di queste risorse, che non esistevano prima che quelle regole fossero definite. Questa è la sfida che impegna.

Cercherò assieme a voi di ripercorrerne i momenti principali, ma so che in ogni convegno queste nozioni vengono offerte. Proverò semplicemente a ricordare la base di partenza e a ripercorrere le modalità con le quali la normativa si è organizzata per governare, si fa per dire, il fenomeno che ci impegna.

In proposito, possiamo premettere che l'atteggiamento delle autorità è sempre stato difensivo, sostenuto dall'idea che esiste una struttura economica con valori conosciuti e ogni volta che questa struttura si interfaccia con questa nuova realtà virtuale è necessario riconoscere chi muove risorse all'interno della realtà tradizionale. Viene utilizzata la figura della cinta daziaria: dal momento in cui qualcosa entra o esce dal mondo dell'economia classica bisogna immaginare che qualcuno controlla, chiede conto di che cosa si sta facendo e per quale motivo. E infatti i primi soggetti tenuti a collaborare sono stati, appunto, gli *Exchange*. Ma quali? Quelli che convertono le valute virtuali in moneta fiat, avente corso forzoso. Questo è il primo momento: siamo nel 2017 in Italia e siamo stati abbastanza all'avanguardia. Solo questi operatori erano tenuti a obblighi di collaborazione antiriciclaggio nel particolare momento della conversione, non ancora in quello della custodia. E questo perché? Perché nelle valutazioni delle autorità internazionali non era emerso un quadro normativo definitivo omogeneo. Guardate qual è la posizione della maggior parte dei Paesi negli Stati Uniti, dei Paesi nordamericani, dell'Europa occidentale. Noi abbiamo un fenomeno accettato, ma con ampie aree non

disciplinate. Negli Stati Uniti, ad esempio, non esiste una legge federale che disciplini la materia, ma abbiamo leggi statali che fanno passi avanti. Lo Stato di New York è uno di questi, il Delaware immagina applicazioni per le annotazioni delle quote nell'ambito delle strutture societarie; poi abbiamo delle realtà diversificate, ad esempio in Germania le criptovalute sono unità di conto e strumenti finanziari. L'attribuzione della qualità di strumenti finanziari è di grande significato, perché nel momento in cui si opera una qualificazione in questi termini scattano presidi; senza quella qualificazione, quei presidi non possono scattare. Pensate alle forme di abusivismo nella proposta, nella sollecitazione all'investimento in qualcosa che viene considerato, o meno, strumento finanziario. Si può immaginare una tutela del risparmiatore, come per la proposta di investimenti in alcune criptovalute, per cui spiegare le caratteristiche di volatilità della risorsa significa rendere avveduto il cliente, l'investitore dei possibili rischi; viene in rilievo, poi, tutta la disciplina di rapporto con l'autorità di vigilanza piuttosto che la disciplina del prospetto informativo da emanare prima di mettere sul mercato un prodotto finanziario da investimento.

In Germania questo è stato possibile nella misura in cui l'ordinamento si è fatto carico di dire: "*Quale è la funzione fondamentalmente per cui uno compra o acquista criptovaluta?*"; così è stata colta l'ottica, riconosciuta a livello normativo, per cui la causa di questo acquisto è tendenzialmente quella di investimento, di speculazione, intendo dire di acquisizione di un guadagno, non necessariamente un incremento della propria risorsa. La Francia è ancora su posizioni di attesa. Alcuni Paesi sono restrittivi. La Russia predilige un atteggiamento contrario, salvo poi immaginarne un controllo su base statale. Altri Paesi hanno intensificato i controlli: la Cina, in maniera paradigmatica, ma anche la Corea del Sud. Le autorità internazionali, parliamo del Fondo monetario, sono molto caute. In generale prevale l'impostazione casistica, cioè la criptovaluta è una sostanza multiforme ed è la funzione che determina la disciplina giuridica. Ad esempio, la SEC, cioè l'autorità di controllo della borsa negli Stati Uniti, ammette anche che possano avere valenza di strumenti finanziari, ma solo all'esito di un'analisi concreta delle caratteristiche identificative dell'investimento finanziario: impegno di capitale, promessa di rendimento, aspettativa di rendimento, rischio. Quando abbiamo questi elementi e tutto torna, allora possiamo immaginare che si sia nell'ambito di questa fattispecie: bisogna però capire quella che nell'elaborazione della Corte di Cassazione, in due precedenti recenti sentenze del 2020 e il 2021, si chiama la causa concreta e che si definisce anche quale funzione economica di un'operazione. Come vi dicevo, l'orientamento è assolutamente diversificato. La

Svizzera ha una disciplina in materia di antiriciclaggio assai severa. Malta ha una disciplina dei servizi inerenti l'utilizzo delle valute virtuali completa e anzi la propone perché aspira a diventare centro attrattivo per una serie di investitori e di operatori.

L'Autorità bancaria europea, l'EBA, ha emesso comunicati, ma si potrebbero definire anche moniti, nel 2012, nel 2015 e poi li ha ripetuti anche recentemente, ricordando i rischi delle valute virtuali; li ripete perché dopo aver fatto questi comunicati i rischi aumentano, come si sperimenta in tutta una serie di casi tratti dalla prassi.

La Corte di giustizia dell'Unione europea nel 2015 ha dato una lettura delle criptovalute rilevante in ambito di disciplina fiscale. Riconoscendo l'operazione remunerata di cambio tra monete virtuali e monete tradizionali quale servizio oneroso significativo ai fini reddituali, l'ha definita esente in ambito IVA, ma pur sempre rilevante. Cosa vuol dire che le relative operazioni siano rilevanti? Vuol dire che devono essere contabilizzate, che devono essere registrate e ne va data una rappresentazione quantunque siano esenti dal pagamento dell'IVA. Questo ha una ricaduta sulla materia penale, perché se l'operazione non produce un'imposta in ambito IVA, non potranno essere ipotizzati i delitti tributari di omesso versamento dell'IVA, piuttosto che di omessa dichiarazione. Peraltro i redditi svolti dagli operatori, i *mining* piuttosto che gli *Exchange*, piuttosto che i prestatori di portafoglio digitale, possono essere a tutti gli effetti equiparati, secondo indicazioni che ci provengono anche da risoluzioni, a redditi di impresa, a ricavi rilevanti, con i costi, alla definizione di una base imponibile rilevante ai fini delle imposte sui redditi. Base riferita a soggetti persone fisiche ma anche a soggetti societari. Questo per dire come poi l'ordinamento cerca comunque di riprendere il governo del fenomeno.

Un'autorità fondamentale nella materia è poi la Banca d'Italia, da sempre fautrice di una lettura assai cauta nella qualificazione delle criptovalute. Cioè se si esamina la definizione normativa della valuta virtuale, la stessa deve molto a indicazioni in negativo che le autorità di vigilanza hanno da subito curato di porre. L'art. 1, comma 2, lettera qq), del decreto legislativo 231/2007, definisce la valuta virtuale "una rappresentazione digitale di valore non emessa e non garantita da una banca centrale o dall'autorità pubblica". Si comincia a definire l'oggetto dicendo cosa non sia: non è emessa e non è garantita da una autorità pubblica e può essere utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalità di investimento. Qui c'è una visione ricognitiva, vorrei dire, priva di entusiasmo ma ricognitiva. L'ordinamento, ancora, non presidia le valute virtuali con garanzie di rimbor-

so. L'esperienza economica, dunque, insegna che può essere utilizzata come mezzo di scambio, come mezzo di investimento, con finalità di investimento. Questa prima disciplina arriva dopo anni dall'insorgere del fenomeno. Le prime discipline non parlavano della finalità di investimento, aggiunta nel 2019, quando l'ordinamento ha preso atto di una funzione economica della risorsa nella realtà.

Una recente normativa, il decreto legislativo 184 del 2021, nel momento in cui ha prestato una tutela penale agli strumenti di pagamento diversi dal contante, vi ha ricompreso la valuta virtuale novellando una norma, l'articolo 493-*ter* del codice penale, in maniera da proteggere anche l'utilizzo indebito di uno strumento di pagamento, che non è riconosciuto per tale dalla Banca d'Italia, ma che esiste, per così dire, nella realtà degli uomini; il diritto penale interviene anche rispetto a queste situazioni e quindi anche l'utilizzo indebito di una valuta virtuale oggi ha un preciso presidio nell'articolo 493-*ter* c.p.

Vorrei sottolineare un dato di portata generale: si è in presenza di una realtà economica che preme sull'ordinamento e quest'ultimo reagisce con gli strumenti che possiede; talvolta "allarga" la portata delle norme, talvolta è necessitato a crearne di nuove. E così se il legislatore inizialmente decide di intervenire nel momento del passaggio attraverso le cinte murarie, poi si rende conto che limitare a questo momento il controllo non avrebbe senso, perché tutto potrebbe rimanere per lunghi tempi in un'area di sospensione restando all'interno dei recinti offerti dai prestatori di servizi virtuali, senza sortirne; perciò, sono stati estesi anche a costoro i doveri di adeguata verifica, di conservazione dei dati, di segnalazione dell'operazione sospette, rendendo anche gli *Exchange* in monete virtuali destinatari di obblighi di collaborazione. Altrimenti cosa potrebbe succedere? Quello che l'esperienza ha insegnato. Vi dicevo prima, l'ipotesi era di un controllo diretto ed esclusivo della risorsa, la stringa alfanumerica, la sostanza informatica della valuta virtuale. Ma in termini economico-sociali la valuta virtuale è una rappresentazione di valore o essa stessa è il valore? A ben vedere se ho la stringa detengo il valore e questo spiega la peculiarità di questa situazione, assimilabile al contante, come diceva il Professore.

Così devo cominciare ad applicare delle categorie diverse, ad esempio il diritto di credito. Verso chi? Se la mia relazione è informatica o crittografica verso la stringa che sostanzia il controllo, non ho credito nei confronti di nessuno; però, se qualcuno gestisce le mie chiavi private perché nell'ambito di quella concreta organizzazione della custodia delle risorse, in realtà le ho cedute, allora nel momento in cui non mi vengono restituite ho certo un credito nei confronti di qualcuno.

Di chi è la proprietà delle risorse nel caso di custodia da parte di terzi della chiave? Nella vicenda che vi anticipavo, l'intera fase prefallimentare ha avuto ad oggetto la definizione di chi fosse il proprietario delle criptovalute. La proprietà delle criptovalute, secondo la lettura che poi il Tribunale e la Corte di appello hanno avallato, era dell'*Exchange*, che aveva il dovere di restituire il *tantundem*. Sapete quale schema contrattuale è stato applicato? Quello del deposito irregolare, anzi di un contratto misto in cui qualcuno si impegnava a fare *trading*, a fare commercio, costruito sulla base del deposito irregolare, del quale sono state applicate le regole in punto di responsabilità del depositario. Cosa succede quando c'è un deposito regolare o cosa succede quando c'è un deposito irregolare? Se il deposito è regolare non interessano i motivi della scomparsa della risorsa, ma che venga restituito il bene affidato; se questo fosse stato il patto, la condizione di esonero dalla responsabilità del depositario sarebbe stata quella di denunciare prontamente la sparizione. Quindi se voi mettete, scusate la banalizzazione, le scarpe nell'armadietto, avete il diritto di riavere le scarpe e non certamente il *tantundem*, salvo però che vi spariscano e il depositario, avvedutosi, non vi dica nulla a tempo debito; situazione che apre a prospettive risarcitorie. Nel momento in cui avete un deposito irregolare, invece, e vi spariscono le scarpe, avete il diritto di avere un altro paio di scarpe o un valore corrispondente.

Perché siamo ricorsi a questi approfondimenti? Perché abbiamo cercato di capire come funzionava la custodia, sia in termini tecnici che contrattuali, superando l'idea astratta di una custodia non intermediata.

Noi viviamo, del resto, in un mondo straordinariamente intermediato. La comune condizione dell'uomo è quella di usufruire e offrire servizi in favore di altri, servizi per lo più remunerati, con tutto quello che consegue. Occorre coltivare una visione complessa di questa realtà. I sistemi economico-sociali e tecnologici non vivono puri, vivono nella condizione multiforme in cui la fanno vivere gli uomini. Alcune persone hanno perso il *Bitcoin* che avevano comprato, si disperano, non riescono a trovare le chiavi e dicono: "*Accidenti, se avessi affidati a un* Exchange *le chiavi del* bitcoin*, oggi sarei nella condizione di riaverlo*". Così, con l'*Exchange* tornano le regole della fiducia, a scapito però dell'esclusività del controllo, come prima ben spiegava il Professore.

Prof. Francesco Bruschi: Trovo interessante il discorso delle responsabilità individuali riconnesse a tali tecnologie. C'è un detto in questo settore: "*Not your keys, not your coins*", cioè se tu non hai le chiavi, i *Bitcoin* non sono tuoi. Il rapporto con gli *Exchange* rappresenta l'attualizzazione di questo principio, nel bene e nel male. Qualcuno ritiene che l'estrema respon-

sabilità posta in capo all'individuo sia addirittura insostenibile. La domanda è: cosa accadrà se questi strumenti raggiungeranno nella loro forma più pura, quella decentralizzata e autonoma, le masse ovvero la maggior parte dei consumatori? Per alcuni la responsabilità di custodire queste chiavi è troppo alta: se ho queste chiavi (e poi vediamo come facciamo a custodirle) le posso perdere, come capita. Sembrerebbe inevitabile l'alternativa di affidarsi a professionisti, salvo gli arbitrii dei quali si possono rendere responsabili e dei quali abbiamo parlato. In realtà, sono allo studio soluzioni più complesse tecnicamente, ma anche più accessibili, che mirano a configurare diverse architetture di custodia che, per esempio, funzionano così: invece di dovermi segnare la chiave del *wallet* su un pezzo di carta, metterla in cassaforte, assicurarmi che non si bruci, eccetera, uso questa accortezza: genero un *Wallet* e poi nomino (attenzione, tutto questo sempre sulla *blockchain*) un certo numero di cosiddetti *guardian*. Per esempio, posso nominare lei, posso nominare il mio collega Vincenzo Rana. Che ruolo hanno questi *guardian*? Nel momento in cui perdo le chiavi, i *custodian* possono intervenire per cambiare la chiave di controllo e questo è un meccanismo che non è né "*Not your keys, not your Bitcoins*" (perdo la chiave ho perso tutto), né attribuisco a lei o agli altri *guardian* i poteri che oggi hanno gli *Exchange* centralizzati, perché il *guardian* ha solo il potere, in determinate condizioni, di aiutarmi a recuperare il controllo dei miei beni. Quindi si stanno sviluppando soluzioni tecniche, con implicazioni non tecniche, che mirano proprio a colmare questo abisso fra la totale responsabilità in capo all'individuo e invece il totale affidamento a un intermediario che deve essere fortemente affidabile.

Dott. Fabio Di Vizio: Lei vede sempre del bene in ogni prospettiva di sviluppo tecnologico. Io a volte vi scorgo la necessità di monitorare la situazione perché questi intermediari, poi, che caratteristiche di garanzia patrimoniale offrono a tutt'oggi? Noi abbiamo un registro presso l'Organismo degli agenti finanziari e i mediatori creditizi, che dal 16 maggio è entrato in vigore. Quindi c'è un censimento degli operatori. Se uno di questi non si iscrive si espone al rischio di sanzione amministrativa per abusivismo nello svolgimento dell'attività di prestatore di servizi di valuta virtuale. D'altro canto, sappiamo che per svolgere un'attività bancaria o finanziaria l'ordinamento prevede requisiti patrimoniali e di onorabilità particolarmente stringenti, mentre requisiti patrimoniali per svolgere questa tipologia di servizi non vi sono. Tanto è vero che oggi parliamo di disintermediazione bancaria, non nel senso di attività controllata dal cliente, quanto per segnalare che gli intermediari bancari e finanziari classici retrocedono rispetto a una serie di servizi ora presidiati e svolti da soggetti innovativi. Ciò offre prospettive di nuova imprenditoria, ma

al tempo stesso pone problemi all'operatore giudiziario e in particolare anche al Pubblico Ministero e alle autorità di polizia giudiziaria nello svolgimento dei propri compiti. Perché è chiaro che se nel momento in cui l'ordinamento ha immaginato che per svolgere l'attività, ad esempio, di amministratore di un ente bancario bisogna avere una certa professionalità, una certa storia personale e l'assenza di condanne per talune tipologie reati, nel momento in cui ci possono essere schemi di custodia di risorse conseguite con il risparmio sarebbe lecito attendersi che qualcosa di similare possa venir richiesto anche a questi operatori. In realtà l'ordinamento non richiede ancora questo livello di professionalità e di requisiti patrimoniali, per un motivo: perché non intende regolare troppo. Perché regolare troppo potrebbe significare determinare una crisi nell'evoluzione di un fenomeno che tutto sommato evidentemente si apprezza. Stiamo esaminando una realtà, come vi ho detto, multiforme e multivalente, ma che corrisponde a nuove opportunità.

Pensate alle nuove possibilità di finanziamento (*lending*) favorite dalle criptovalute: se fate una ricerca in internet verificherete che è tutto sommato agevole mettere criptovalute a garanzia di un prestito. Ora, in un momento in cui il sistema bancario vive fibrillazioni sui tassi di interesse, si aprono possibilità straordinarie. La domanda: tutto questo merita o no un presidio normativo?

Quello che possiamo dire è che il legislatore si è avvicinato lentamente, e vorrei dire prudentemente, al fenomeno con diverse normative. La prima di esse è quella dell'antiriciclaggio; un'altra intervenuta con buon prontezza è quella sul monitoraggio fiscale, con la previsione per cui in caso di trasferimenti di valuta virtuale all'estero, oltre certe soglie, intermediati dagli *Exchange* sussistono doveri di comunicazione all'Agenzia delle Entrate; inoltre, l'UCIFI piuttosto che il Nucleo di polizia valutaria possono fare interrogazioni per masse, per tipologie di operazioni di valuta virtuale che coinvolgono anche il trasferimento all'estero, sopra certe soglie, e sapere chi sono i titolari effettivi. Questi operatori, in teoria, devono acquisire dati sul titolare effettivo e sulle causali delle operazioni. Un terzo momento nel progressivo riconoscimento normativo del fenomeno si è registrato recentemente, come vi dicevo, con la regolamentazione degli strumenti di pagamenti alternativi al contante; la valuta virtuale è entrata nella struttura di una aggravante della truffa; l'art. 640-*ter* c. 2, secondo periodo, c.p., prevede in forma di aggravante la realizzazione della condotta attraverso il trasferimento di valuta virtuale. Quest'ultima, inoltre, è oggetto materiale della condotta tipica della fattispecie penale dell'art. 493-*ter* codice penale.

L'ordinamento ha poi cominciato a porsi con chiarezza uno dei temi

più importanti: perché si comprano le criptovalute? Le criptovalute sono di tanti generi; le potremmo classificare sotto vari profili ovvero in relazione ai prestatori, al rapporto con l'economia – chiamiamola classica o tradizionale – alla convertibilità o non convertibilità, in un senso o in entrambi i sensi. Quando parliamo dei criptoasset, in senso più ampio per cercare un *genus*, dobbiamo escludere di essere in presenza di uno schema che si ripete necessariamente con lo stesso funzionamento. Giustamente il professor Bruschi ci ha spiegato alcune caratteristiche ricorrenti, però alcune peculiarità sono proprie solo di alcune monete virtuali

Partecipante al Seminario: A proposito della varietà delle criptovalute, le volevo chiedere se, anche approfittando della presenza del professor Bruschi, si può riservare un momento di approfondimento sui *Monero*, che è la criptovaluta più utilizzata dalla criminalità organizzata. Quali sono le caratteristiche tecniche e quali sono gli strumenti che possono utilizzare gli investigatori per cercare di colpire questi *asset*?

Dott. Fabio Di Vizio: Ero in arrivo su questo tema. *Z-cash* piuttosto che *Monero* sono proprio le valute virtuali che offrono peculiari funzionalità rispetto alla piena tracciabilità dei soggetti e delle varie fasi. L'aspetto tecnico lo affido al professor Bruschi e semmai ne potremmo parlare anche nella fase laboratoriale, dove appunto il tema della identificazione dei soggetti e delle singole operazioni sarà il filo conduttore. A volte sentiamo dire che è stata bucata la *blockchain*, evocando l'idea della scoperta dell'identità dei membri di una loggia segreta. Sono affermazioni sostanzialmente improvvide perché resta complicato fare un'indagine di *Bitcoin forensics* alla ricerca delle tracce informatiche. Tenete per chiaro un concetto: un conto è dire che qualcosa è tracciabile, altro è dire che è rintracciabile. La fattispecie del riciclaggio, ad esempio, si configura nella misura in cui si determina un ostacolo all'identificazione della provenienza delittuosa di una risorsa, oggi neanche più delittuosa, perché la riforma del 2021 ha ammesso anche l'origine contravvenzionale. Nell'elaborazione giurisprudenziale il reato è integrato non tanto perché non sono più nelle condizioni di ricostruire la traccia, ma quando sono ostacolato, ovvero è resa complicata l'opera di ricostruzione. Volendo verificare questa caratteristica per le criptovalute è agevole rendersi conto che questa ricorre perché vengono coinvolte più giurisdizioni, vengono fatte delle conversioni, si passa attraverso più *Exchange*, si passa tra diversi *address* all'interno dello stesso *Exchange*: noi tutti ora sappiamo che se si rimane ad esempio nell'ambito di un *Exchange* centralizzato tutto è tenuto nell'ambito della contabilità interna, ma nulla appare fuori. Quindi quale "buco" della *blockchain* potrebbe determinare la scoperta dell'identità dei soggetti coinvolti in un'operazione?

Anzi, questo diventa un "mondo sospeso" nel quale tutto si può nascondere e che impone obblighi di collaborazione al soggetto che gestisce tutto questo. Affido, ora, al prof. Bruschi, di spiegare, più in dettaglio, le caratteristiche tecniche di *Monero* e *Z-cash*.

Prof. Francesco Bruschi: Senz'altro. Allora, l'osservazione è corretta. Abbiamo ricordato che, parlando di *Bitcoin*, ogni movimento di *asset* tra due soggetti è documentato. Noi possiamo andare sulla *blockchain* di *Bitcoin* o di *Ethereum* e verificare, dato ogni movimento, da chi è partito, a chi è arrivato, l'ammontare del movimento. Tutte queste informazioni sono in chiaro. Sono però state sviluppate delle tecnologie crittografiche che consentono di dare le stesse garanzie di integrità che offrono le *blockchain* di *Bitcoin* e *Ethereum* ovvero: il fatto che gli utenti possono spendere solo quello che hanno, che le spese non sono reversibili e che le regole vengono rispettate, senza però svelare alcune informazioni. Quindi se io detengo *Monero*, posso trasferirli a un altro soggetto in un modo che garantisce a qualsiasi osservatore alcune proprietà: chiunque da fuori vede che c'è stato un trasferimento, che questo trasferimento è avvenuto secondo le regole, quindi io non ho speso qualcosa che non avevo e dunque non sono state create nuove monete. Ma da fuori un osservatore non può capire né il soggetto da cui è partita la transazione, né il soggetto ricevente e, recentemente, neanche l'ammontare. Dopo andremo proprio a vedere che sulle *blockchain* come su *Bitcoin* vedo che da questo soggetto parte tot e arriva a tot; invece su *Monero* non lo vedo, ma registro solo transazioni confidenziali, ove scorgo solo che c'è stato un movimento, né di quanto, né da chi, né a chi. Questa cosa è possibile con gli strumenti crittografici che sono stati messi a frutto da qualche decennio. Strumenti veramente affascinanti come le *ring signature*. Ripeto, non entro nei dettagli e ovviamente, se vi interessa, avremo modo di organizzare un approfondimento. Quindi in *Monero* ho questa possibilità. Chi vuole provare a tracciare quei meccanismi induttivi di cui dicevamo prima, capire da dove viene un certo flusso finanziario, a chi appartiene un certo *address*, ovviamente ha le armi estremamente spuntate. Questa cosa è vera, ancora di più in *Z-cash*, perché attraverso un'altra tecnologia crittografica, questa più recente, la cui nascita dobbiamo a un genio italiano che è il professor Silvio Micali, è possibile nascondere queste informazioni ancora di più. Quindi in *Z-Cash* quello che vedo è semplicemente che c'è stata una transazione e null'altro. Che strumenti ho a disposizione per aggredire questa forma di opacità? Qui la storia si fa estremamente più complicata e ci sono pochissime cose che si possono fare. Dal punto di vista investigativo è necessario basarsi su delle operazioni sotto copertura, quindi infiltrare degli agenti economici.

Dott. Fabio Di Vizio: Naturalmente laddove la normativa permette questa tipologia di attività, su questo bisogna essere molto attenti. Ecco però lei tecnicamente dice come possiamo risolverlo? Li provochiamo.

Prof. Vincenzo Rana: Sì, bisogna infiltrarsi perché dal punto di vista dell'analisi ci troviamo di fronte a un muro impenetrabile. La situazione non è del tutto dissimile da quanto avviene quando abbiamo a che fare con reti private di soggetti, quindi di VPN, meccanismi crittografici di occultamento dell'informazione. Voi sapete che crittograficamente queste strutture sono impenetrabili e quindi in quel caso si utilizzano gli strumenti che voi conoscete meglio di me, ma che io sommariamente, dal punto di vista tecnico, chiamo infiltrati, chiamo azioni sotto copertura. Purtroppo, questa è la realtà.

Partecipante al Seminario: L'attività organizzata transnazionale usa questi strumenti e li usa perché tecnicamente è possibile, ma non si possono fare accordi internazionali con i quali questi strumenti di pagamento vengono sottoposti a regole, a normative, doveri di tracciabilità? Cioè, possibile che tutto deve essere lasciato in mano ai tecnici che sono in grado di fare quello che vogliono e non si può vincolare, non si possono mettere paletti normativi?

Dott. Fabio Di Vizio: Volendo tradurre altrimenti la sua sollecitazione dovrei dire: "*Bisogna o no adesso regolare il fenomeno?*", perché questo è fondamentalmente quello che lei dice. Ormai c'è una generale condivisione delle opportunità di farlo anche per quelle considerazioni che lei introduceva, ma anche per quelle più normali, proteggere nuovi bisogni di tutela. Ho esordito nell'esposizione dicendo qual è stato l'atteggiamento tradizionale: difensivo, ossia volto a proteggere l'economia, gli strumenti e i valori economici tradizionali allorché si interconnettono con gli altri. Soltanto che questa prospettiva funziona se il fenomeno virtuale non rappresenta un vero e proprio ecosistema complesso e articolato, vale a dire quando è qualcosa del tutto residuale, minimo e non significativo. Oggi definire "non significativo" qualcosa che, già qualche mese fa, ha avuto valori di patrimonializzazione pari a circa 3.000 miliardi (l'equivalente di tutto il risparmio bancario delle famiglie italiane), che significa cinque o sei volte i valori del bilancio dell'Unione europea in materia di spesa sanitaria, è un po' riduttivo. La mia è, però, una valutazione *de iure condendo*. Stando ai dati normativi attuali, abbiamo i tentativi di classificazione o di interventi che però, obiettivamente, come vi accennavo già in apertura, avvengono a macchia di leopardo. Per i tedeschi sono strumenti finanziari, come per parte degli Stati americani, per altri non lo sono e non devono esserlo. Quelle pronunce della Corte di Cassazione, che poi rapidamente passerò in rassegna, intervenute tra il 2020 e il 2021, hanno ritenuto che in alcuni casi l'offerta di moneta virtuale possa integrare un pro-

dotto finanziario e quindi hanno ipotizzato la configurabilità della fattispecie di abusivismo sollecitatorio; ma sono state tacciate di cripto-analogia, cioè di un'inammissibile operazione interpretativa con cui realizzata una inammissibile estensione della norma penale. Ora, per fortuna, la Corte di Cassazione ha le spalle larghe, però questo testimonia come il tema ancora oggi sia controverso, per riconoscibili margini di opinabilità.

Vorrei con voi cercare rapidamente di concludere la spiegazione in negativo della criptovaluta, ovvero quello che il legislatore nega che possa essere: non è moneta, perché non ha corso legale e forzoso; cioè se io voglio pagare con una valuta che ha corso legale, posso pagare e liberarmi, ha potere liberatorio, satisfattorio. Invece, non posso costringere nessuno a ricevere il prezzo in *Bitcoin* piuttosto che in altra valuta virtuale. Quindi questo è il primo elemento. Noi continuiamo a parlare di monete e valute virtuali, però. Anche lessicalmente, nonostante dovremmo forse parlare più correttamente di *cripto-asset*, ci rendiamo conto che in concreto, non di rado, la loro funzione è divenuta quella di consentire il pagamento su base convenzionale. Certo che se non è valuta, non si applica la disciplina valutaria delineata dal d.lgs. n. 195/2008. Se non è valuta non si applica per i passaggi in frontiera o in dogana la disciplina valutaria prevista per il trasferimento al seguito.

Partecipante al Seminario: Volevo chiedere, ritornando al caso pratico che lei prima ha prospettato del fallimento del gestore della piattaforma di scambio e custodia di criptovalute: in quel caso come è stato legittimato il creditore nel fallimento?

Dott. Fabio Di Vizio: Non posso entrare nel dettaglio perché è un caso giudizialmente ancora aperto per la parte penale, anche se la vicenda fallimentare si è chiusa con una pronuncia definitiva. Mi limito all'aspetto tecnologico, nulla di più. Naturalmente è stata creata una massa fallimentare ed uno stato passivo ricevendo le domande di insinuazione dei creditori. Però, in sostanza, è stata posta una problematica dai creditori, gli *users,* molti dei quali non volevano la conversione delle criptovalute, invece realizzata; l'*Exchange* non aveva una sola criptovaluta, aveva tante criptovalute; per lo più i *Bitcoin* sono stati convertiti e questa è stata una scelta dei curatori, sostenuti dal giudice delegato, che a un certo punto hanno detto: "*Va bene, fermiamo la situazione ad una certa data e convertiamo, creiamo massa fallimentare ripartibile*"; nondimeno, alcuni degli *users* hanno opposto: "*Ma noi abbiamo investito in quella risorsa e vogliamo avere quella risorsa, il mio saldo era rispetto a quella risorsa virtuale, non nella criptovaluta non restituibile, vogliamo le nostre criptovalute*". Il problema è stato risolto nel senso che tutto è stato convertito in massa fallimentare, ma è stata un'operazione non scevra da margini

creativi in un quadro normativo carente. Il tribunale ha ritenuto più adeguato convertire tutto in moneta *fiat* e ripartire secondo i valori del momento in cui non era più stato possibile ritirare alcune valute virtuali. Quindi si è definito un parametro temporale di ragguaglio. Quindi, come vedete, abbiamo spesso davanti scelte importanti da assumere per tutelare risparmiatori e creditori, in un quadro normativo non di rado evanescente.

Lo stesso sequestro di criptovalute, poi ve lo spiegheranno meglio gli ingegneri, ha implicato scelte complesse e innovative: non è facile sequestrare criptovalute, cioè mettersi nelle condizioni di escludere qualcun altro con sicurezza dalla possibilità di venirne in possesso. È stato creato un nuovo protocollo informatico per cercare di custodire quelle risorse in maniera riservata. Con la preoccupazione, fino a che questa operazione non è andata a buon fine, che qualcuno, a conoscenza delle chiavi di controllo delle criptovalute, potesse riprenderne le disponibilità. Sono state svolte attività di perquisizione, di sequestro, azioni di inibizione della possibilità di entrare in un certo *address*, ma se poi il soggetto fosse riuscito, avendo il controllo in maniera più o meno corretta e da remoto, a utilizzare le chiavi, avrebbe di fatto potuto vanificare il vincolo. Questo per dirvi quanto la conoscenza delle base tecnologica in questa materia sia imprescindibile. Del resto, l'informazione tecnologica ci porta a dire che ci sono tanti schemi, tante *blockchain*, non abbiamo una sola *blockchain*. Ingegnere, mi aiuta su questo?

Prof. Francesco Bruschi: È corretto. Dal punto di vista tecnico abbiamo tante *blockchain*; il caso cui si riferisce incideva su diverse *blockchain* e a diverse *blockchain* corrispondono anche diverse modalità tecniche di intervento per esempio per il sequestro. Quindi è del tutto possibile togliere la disponibilità dell'utilizzo degli *asset* in questo caso. Normalmente nel farlo è necessario oltrepassare il paradigma in cui ci si affida a un intermediario: se devo congelare un conto corrente bancario, lo dico alla banca e la banca obbedisce assumendone la responsabilità. Qui, invece, anche chi conduce le indagini deve fare da solo, accettando il fatto che le garanzie vengono date dalla crittografia e questo, mi rendo conto, può essere destabilizzante. Quindi se in passato per congelare un conto potevo rivolgere l'ingiunzione alla Banca, trasferendole la responsabilità, in questo caso devo attrezzarmi per eseguire il trasferimento su un dispositivo di cui conosco e controllo le chiavi. La responsabilità a chi è in capo? Chi detiene quelle chiavi? Come vengono custodite? Mi rendo conto che queste siano problematiche e che questo paradigma possa destabilizzare.

Dott. Fabio Di Vizio: Vi faccio un esempio, plastico, e anche su questo mi aiuterà l'ingegner Rana, perché è bravissimo. Ci siamo posti a un certo

momento un problema conseguente al fatto che le chiavi private controllano la risorsa. Voi pensate a un sequestro oppure a un passaggio su un'altra piattaforma di queste risorse, ma in cui i curatori controllano la risorsa e pensate cosa significa prendere il controllo per il curatore. È stato necessario dividere le chiavi e diversificarle, in maniera da non porle sotto il controllo di una persona sola, perché quello di cui stavamo parlando era un valore assai consistente. Parliamo di un centinaio di milioni di dollari. Pensate al caso di una persona con una chiave che controlla in esclusiva 100 milioni di dollari. E quindi bisogna anche immaginare come impedire a questa persona di avere una disponibilità esclusiva della quale possa abusare. Perché non è stato il caso di specie, che registrava solo galantuomini, ma se costoro si fossero imbarcati in un volo verso un'isola deserta in cui poter spendere questa criptovaluta, come capita adesso in un paio di Paesi dell'America centrale, ci saremmo trovati dinanzi ad una perdita irreversibile delle risorse. Insomma, sono problemi che si devono gestire e quando è stato creato questo protocollo si è dovuto tener conto di come funzionava la base tecnologica.

Prof. Francesco Bruschi: Qui, dottore, mi lasci una piccola puntualizzazione. Una cosa che si può fare, che si fa, che forse è impossibile non fare in questi casi, è dare il controllo crittografico di una risorsa non a un soggetto, ma a un insieme di soggetti attraverso un meccanismo cosiddetto *N-out of-M* e quindi posso trasferire gli *asset* su un indirizzo controllato non da una persona singolarmente ma da un insieme di persone che devono concordare. Per esempio, qui posso realizzare diverse architetture, per esempio 3 su 5. Allora faccio in modo di distribuire le responsabilità su 5 persone, in modo che per trasferire ci voglia il consenso di almeno 3 di queste 5 persone. Questo chiaramente ammorbidisce molto la cosa perché a questo punto posso anche sequestrare uno di questi soggetti, per configurare un'altra possibilità spaventosa, ma lui da solo non può fare niente, quindi ne devo sequestrare tre. Lui può sfuggire comunque voglia, ma gli altri si possono attrezzare, purché ne rimangono ovviamente 3 su 5. In questo particolare caso, che appunto è stato un caso anche dal punto di vista *forensi*c del tutto innovativo in Italia, era stato utilizzato un meccanismo *multisignature*.

Dott. Fabio Di Vizio: Io l'avevo un po' drammatizzata, confesso, ma in realtà la tecnologia aveva anche aiutato rapidamente a lenire le preoccupazioni.

Torniamo ai nostri problemi di qualificazione giuridica. Abbiamo detto che la criptovaluta non è moneta, non è valuta. Però, ad esempio, l'Agenzia delle Entrate la considera valuta straniera e ritiene che sia esente IVA; per definire eventualmente le plusvalenze, realizza una tassazione che va para-

metrata al regime che si applica alle valute straniere quando hanno giacenze sopra i vecchi 100 milioni di lire, circa 51 mila euro, per 7 giorni consecutivi. Adesso non sto a entrare troppo nei dettagli.

Non è moneta elettronica, perché? Voi direte "ma come! è moneta elettronica per definizione" e invece no, perché il legislatore definisce la moneta elettronica in relazione alla sua emissione in cambio di fondi corrispondenti a valuta reale; per contro, la criptovaluta non ha corrispondenza con la valuta reale, mentre la moneta elettronica deve essere rimborsabile/convertibile in valuta reale, condizione non necessaria per tutte le criptovalute.

È moneta complementare? Le monete complementari sono forme sperimentate in piccole realtà per favorire il commercio e le realtà economiche di limitati ambienti comunitari, ma la criptovaluta ha quale caratteristica identitaria quella di riferirsi ad una realtà globale.

È bene giuridico, direte voi. Abbiamo trovato la norma, cioè l'art. 810 del codice civile: siamo tranquilli, c'era da tempo, e quindi è patrimonio. Che sia patrimonio sarei abbastanza tranquillo, sul bene giuridico qualche riflessione civilistica potrebbe ostacolarlo, perché si potrebbero dover riconoscere che i diritti di esclusiva sui beni, anche immateriali, sono tipici, cioè il legislatore dovrebbe intervenire, definire, riconoscere espressamente. Questo il legislatore lo fa per riflesso, cioè non ci dice cos'è la valuta virtuale ma ci dice cosa non è la valuta virtuale e attraverso questo meccanismo indiretto riesce a dare un valore, un presidio di carattere normativo e consente di dire che è bene giuridico. Il tribunale fallimentare di Firenze ha definito le criptovalute beni giuridici e li ha annessi alla massa fallimentare ai fini della liquidazione.

È documento informatico? In effetti, la valuta virtuale più che rappresentazione di fatti, atti o dati giuridicamente rilevanti è valore. Prima, correttamente, l'ingegnere ci ricordava "guardate che qui il passaggio creativo non sta nel trasformare e trasferire un'informazione, ma nel trasferire qualcosa che è valore", e il documento informatico non ha questa caratteristica.

È mezzo di pagamento? No, non lo è nella misura in cui collide con la definizione normativa che non vi ricomprende la valuta virtuale.

È strumento o prodotto finanziario? Allora, qui il legislatore non dice nulla di espresso. È intervenuta la Corte di Cassazione nel 2020 e ha detto che a certe condizioni la criptovalute sono prodotti finanziari. Nel momento in cui ha fissato questo concetto ha ammesso che poteva essere operante una certa norma penale, l'art 166 del TUF. Cosa dice la Corte, nella pronuncia 26807 del 2020? Che la vendita online di moneta virtuale *Bitcoin* pubblicizzata quale forma di investimento per i risparmiatori, offrendo agli stessi informazioni sulla redditività dell'iniziativa, è attività soggetta agli adempimenti previsti

dalla disciplina degli strumenti finanziari, quindi l'articolo 91 e seguenti del Testo Unico. Se non si realizzano questi adempimenti, è integrato un abusivismo sollecitatorio. Il modo con cui viene reclamizzata la vendita determina la riconduzione alla categoria del prodotto finanziario. Che cosa diceva il sito? "*Chi ha scommesso in Bitcoin in due anni ha guadagnato più del 97%*", cioè valorizzava la redditività di questa tipologia di investimento, e questo è stato sufficiente per definirlo prodotto finanziario. Ma quanti siti hanno questa caratteristica? Fate una ricerca anche qui in Internet e vi renderete conto di quanto è frequente e quanti sono i provvedimenti di sospensione che Consob deve, non dico quotidianamente, ma certamente quasi ormai mensilmente, realizzare per ricordare questo tipo di situazione. Nella sentenza 44337 del 2021, ponendo attenzione alle finalità della condotta di acquisto, si è venuti alla stessa conclusione: qui non è tanto il lato di chi offre, ma di chi acquista a risolvere in problema qualificatorio. Cosa dice la Corte? Che il *Bitcoin* è prodotto finanziario qualora lo si sia acquistato con finalità di investimento. Ditemi se nella nostra esperienza questa finalità di investimento ricorre o non ricorre; avrete, così, l'idea prospettica di quanto questo tipo di affermazione determina l'applicazione di una serie di fattispecie. Se ricorre l'abusivismo nella sollecitazione, ricorrono poi una serie di guarentigie che devono scattare a tutela degli investitori della correttezza dell'informazione.

Infine, qualche considerazione su alcuni soggetti nei quali potreste imbattervi per ragioni investigative: gli Exchange centralizzati di fatto. Noi abbiamo in realtà collettori che sono *users* che hanno esperienza nel settore e ricevono per conto di altri, secondo un meccanismo fiduciario. Il collettore è un custode fiduciario, che si sottrae, attraverso questa nascosta interlocuzione diretta con gli *users*, ai doveri di trasparenza. Vi sono state esperienze in attività di indagine nelle quali l'*Exchange*, intendo un *Exchange* ufficiale, formalmente riconosciuto, presente con buona autorevolezza e onorabilità di comportamenti, aveva però disponibilità tradizionali *fiat*, a sé intestate, che erano di fatto riferibili ai propri operatori. Perché quando si deve operare in un *Exchange* probabilmente è anche necessario avere la possibilità di investire e disinvestire in moneta tradizionale; così si realizza spesso uno schema tecnico che consiste in un conto *omnibus*, in cui tutto viene riversato. Siccome gli *Exchange* non hanno doveri di comunicazione, salvo che all'intermediario presso cui operano, questo significa che nelle disponibilità di un *Exchange* possono finire disponibilità tradizionali ignote all'Agenzia delle entrate perché non oggetto delle trasmissioni periodiche dei saldi dei conti correnti. Voi capite quanto questo complichi un'attività investigativa e quanto imponga di conoscere come i meccanismi funzionano realmente? Una sfida continua.

Passo, infine, al tema dei reati rispetto ai quali è stata sperimentata la strumentalità dell'impiego delle criptovalute. Il riciclaggio, da questo punto di vista, ha un sufficiente spazio di elastica praticabilità perché l'oggetto materiale e l'oggetto della riconversione possono essere pur sempre utilità, nel cui concetto rientra ogni vantaggio economico. Forse non abbiamo ancora capito esattamente cosa sono le criptovalute, ma abbiamo compreso sicuramente che sono un valore economico; ne consegue un tranquillo inquadramento nella rete della fattispecie e questo è una delle ragioni per cui le iniziative investigative sono praticabili, almeno sotto questo profilo. Vi dicevo, prima, che la questione non è tanto quella della tracciabilità ma della rintracciabilità e noi abbiamo una serie di servizi che invece vengono utilizzati contro la tracciabilità. Nell'esempio che facevamo prima, non sappiamo chi fosse l'intestatario del conto, Fabio Rossi, Pippo e la stringa alfanumerica. Noi abbiamo la stringa alfanumerica e prima di arrivare a capire chi c'è dietro la stringa alfanumerica dobbiamo compiere indagini impegnative. L'esperienza concreta di trasferimenti di somme considerevole, utilizzando disponibilità presso intermediari stranieri che a loro volta utilizzano rapporti privilegiati con alcuni *Exchange*, è ormai consueta. Interrompo qui l'illustrazione delle qualificazioni giuridiche che potrebbero essere ancora diverse; potremmo ragionare degli artt. 615-*ter* e 615-*quater* c.p., o dell'art. 494 c.p., potremmo ragionare addirittura del furto con ulteriori problematiche di qualificazione. Incombe il tempo fissato per il laboratorio.

3. Il laboratorio

Dott. Fabio Di Vizio: In questa porzione della sessione vorrei cercare di trasmettervi la necessità di smitizzare le possibilità offerte agli inquirenti ma anche di non perdere la speranza che la traccia del crimine possa concretamente ed utilmente ricostruirsi. Questo, del resto, è il primo disincentivo rispetto a un impiego esclusivamente o elettivamente criminale di questi valori economici. Affido al professor Bruschi la conduzione dell'esperimento laboratoriale.

Prof. Francesco Bruschi: Grazie. L'intenzione è di svolgere questa parte laboratoriale puntando alla speranza che non deve mancare mai. In questa porzione finale la nostra speranza, il nostro obiettivo, è di rappresentarvi concretamente l'utilizzo di alcuni strumenti, qualcosa che nella nostra esperienza didattica e pedagogica, risulta sempre illuminante. Un conto sono le *slide*, un conto, invece, è metterci le mani; quindi, quello che vi proponiamo

è di metterci le mani. Vi faremo vedere l'utilizzo di alcuni strumenti a vostra disposizione, in quanto dotati di un computer, dei *browser*. Vi faremo vedere come tramite un *browser* sia possibile creare un *Wallet*, una di quelle identità crittografiche delle quali parlavo all'inizio, ricevere degli *asset*, degli *Ether*, nel caso di specie, come sia possibile custodirli, trasferirli, tracciarli e provare a occultarne la tracciabilità.

Allora la prima cosa che farei, Vincenzo, è quella di mettermi nei panni di qualcuno che ne ha sentito parlare oggi per la prima volta e dice "*voglio creare una di quelle famose identità crittografiche e poi voglio un po' sperimentare*", magari voglio trovare qualcuno che mi manda un *Ether*, mezzo *Ether*, e poi voglio vedere che cosa ne posso fare, come lo posso trasferire, e poi magari voglio tracciare questi trasferimenti sulla *blockchain*. Allora, il punto da cui partiremo sarà proprio il *Wallet*, quindi installeremo uno di questi programmi che un individuo può creare autonomamente. Tutte queste cose le facciamo con l'ausilio di un *software*. Attenzione, qualcuno potrebbe dire: "*Ah, ma allora sto andando sul sito di un gestore e quindi lui è un intermediario, o lui è comunque qualcuno che può negarmi successivamente l'accesso*". No, questo è un *software* che gira rigorosamente sul nostro computer, che ovviamente possiamo controllare pienamente senza che nessuno ci imponga di far girare quel *software* piuttosto che un altro. Il *Wallet* che andremo a caricare è il più diffuso in ambito *Ethereum* ed è *Metamask*. Se volete seguirci, potete andare all'indirizzo *https://metamask.io* e vi troverete su questa pagina sulla quale si trova Vincenzo e poi potrete scaricare il nostro *Wallet* che, in questo caso, viene sotto forma di un'estensione del *browser*. Questa è una forma tecnica in cui *Metamask* si presenta, in realtà esiste anche come applicazione per il telefono. A questo punto installiamo, quindi clicchiamo su *Install Metamask* e veniamo rediretti alla pagina del *software* e lo possiamo aggiungere a *Firefox*.

Adesso, Vincenzo clicca su "inizia", ci viene data un'opzione: ovviamente adesso andremo a creare un'identità crittografica. Poi, una volta che l'avremo creata, quella resta sul computer che abbiamo creato, ma se noi volessimo portarla su un altro dispositivo, dovremmo poterlo fare. Allora, come vedremo, è possibile creare una copia della chiave privata e portarla da un'altra parte. Ovviamente, se è possibile questo, deve essere possibile, su un altro computer, importare un'identità già creata altrove. Questo è quello che ci viene chiesto: *Metamask* ci chiede "*hai lanciato metamask, ma vuoi importare un'altra identità o ne vuoi creare una nuova?*". Siccome noi siamo dei neofiti totali, vogliamo crearne una nuova, quindi clicchiamo su "*crea un portafoglio*". Ora, qua ci vengono date delle rassicurazioni ("*Metamask è un*

software che funziona, non lo useremo per tracciarti, ecc"), acconsentiamo. Qua mi viene chiesta una *password*, ma uno potrebbe dire "*ma perché la password? nello schema che mi hai detto la password non c'era più*". Qui la *password* verrà utilizzata per memorizzare in modo cifrato e sicuro la chiave privata, cioè verrà creata una chiave privata che sarà quella che ci consentirà di agire, però che succede se mi rubano il computer, me lo sequestrano, leggono la memoria e trovano la mia chiave? Vuol dire che possono accedere ai miei fondi.

Qui c'è un ulteriore passo di sicurezza che non è centralizzato, in cui inserisco la *password* e con la stessa la chiave privata verrà cifrata. Quindi, se anche mi rubano il computer non potranno rubare la chiave anche analizzando la memoria. Ovviamente bisogna usare una *password* sicura. Andando avanti, abbiamo un video che ci racconta un po' dei rischi delle cose che dobbiamo fare, direi di saltare direttamente questa parte.

Ecco qua abbiamo creato la nostra identità crittografica, il nostro conto, abbiamo già l'equivalente, in termini di funzionalità, di un conto corrente bancario: abbiamo il nostro Iban, che è quello che vedete sotto *account 1*. Lì c'è una stringa lunga, possiamo copiarla. Quindi siamo attivi, siamo pronti per ricevere qualsiasi ammontare di asset. In questo caso siamo sulla rete *Ethereum* quindi *Ether*, quindi possiamo farci mandare qualche milione di dollari direttamente senza dover fare altro. Ora vogliamo un po' giocare, non ci basta creare questa identità. Faccio notare come a Vincenzo non sia stato chiesto nulla di niente sulla sua identità, sul nome, neanche sulle *email*. Non gli è stato chiesto alcun riferimento di aggancio ad un'identità esterna a questo mondo che non sia quella crittografica. A questo punto potremmo divertirci: se qualcuno avesse qualche *Ether* da mandare a Vincenzo potrebbe mandarglielo.

Partecipante al Seminario: Scusate, mi sono perso un passaggio, ma la chiave dov'è?

Prof. Francesco Bruschi: La chiave privata è stata generata dal software che la tiene ben nascosta. La chiave privata deve essere nascosta. Noi non la utilizzeremo mai personalmente direttamente, quindi non ci interessa conoscerla. Il *software* ce l'ha in memoria, cifrata. Attenzione qualcuno potrebbe dire "*no, ma io voglio essere assolutamente padrone del mio destino, voglio vederla questa chiave privata, perché per esempio voglio portarmela su un altro Wallet*", lo possiamo fare. Adesso Vincenzo lo farà, ma facendo una cosa che comprometterà irrimediabilmente l'indirizzo che sta usando, facendovi vedere la chiave privata. Infatti, una volta che altri conoscono la sua chiave privata possono impersonare Vincenzo; in particolare, possono impersonare

questa chiave pubblica, quella che vedete qua. Questa è la chiave pubblica, quindi è l'IBAN di Vincenzo e lui non ha nessun problema a farlo vedere, così come voi non avete alcun problema a mostrare il vostro IBAN, perché non è che conoscendo il vostro Iban si può agire sul vostro conto ma vi si può solo inviare del denaro. Adesso Vincenzo, cliccando "*esporta chiave privata*" comprometterà il sistema. Eccola qua, la chiave privata. A questo punto chiunque di voi con questi numeri potrà d'ora in poi controllare pienamente la chiave pubblica di Vincenzo. Questo ovviamente vuol dire che la chiave pubblica la useremo solo a fini completamente didattici. Purtroppo, questo mi impedisce di dare seguito alle esortazioni di mandare degli Ether a Vincenzo perché sarebbero immediatamente oggetto di distrazione. Quindi attenzione, non fatelo se poi avete intenzione di mantenere la vostra chiave.

Per giocare un pochino senza soldi veri abbiamo la possibilità di utilizzare una cosiddetta rete di test, ovvero una piattaforma del tutto analoga funzionalmente a *Ethereum*, ma in cui gli *asset* hanno pochissimo valore, non hanno quasi valore: sono i soldi del Monopoli. Qui, per il resto sono assolutamente uguali: tutto quello che faremo d'ora in poi sarà del tutto identico a quello che si fa con quei soldi veri, però i soldi non saranno veri. Per accedere a questa rete di test dovete cliccare su *show hide*, dovete andare prima su rete principale, si apre questa finestra, cliccate su *show hide* e poi a questo punto c'è questo interruttore *show test networks* che è su *off* lo mettete a *on*. Dopo aver fatto questo, vedrete che nel selettore potete scegliere delle altre reti di test su cui possiamo andare a giocare. Devo sceglierne una, scegliamo quella gialla che si chiama *Rinkeby*. Quindi chiedo a tutti voi di andare sulla rete *Rinkeby*. Il nostro conto su questa rete è nuovo, quindi non abbiamo niente, non abbiamo nessun *token*. A questo punto potrei molto generosamente dare qualche *token* a Vincenzo sulla rete. Come faccio a fare questa trasmissione? Voi adesso non la vedete perché è sul mio computer, ma io apro il mio *Metamask*, il mio *Wallet*, e sulla rete *Rinkeby* ho un po' di disponibilità che trasferirò a Vincenzo, una generosa somma. Come faccio io a trasferirli a Vincenzo? Ho diversi modi. Lui mi può mandare via *Whatsapp* la chiave pubblica, oppure se ho il *Wallet* sul telefono posso usare questo *QR code* molto comodamente. Adesso noi abbiamo *Whatsapp* aperto, posso andare a vedere la *chat,* mi prendo la chiave pubblica di Vincenzo e gli mando un *Ether*. Vincenzo dovrebbe riceverlo. Aspettiamo il tempo tecnico che la mia transazione venga registrata dalla rete.

Colgo l'occasione per dire che quando io mando la mia transazione nella rete, questa viene presa dai validatori, viene aggiunta, ed ecco qua arriva l'*Ether*. A questo punto Vincenzo è ricco, vedete di quanta generosità sono

stato capace, adesso lui che cosa se ne fa di questi *Ether*? La cosa interessante sarebbe che li girasse a qualcuno di voi. Ora noi in qualche misura dovremmo poter ricevere l'indirizzo di qualcuno di voi, almeno di uno di voi, che poi potrà procedere a sua volta a trasferire ai colleghi.

Ci sono diversi modi, non so se voi avete accesso alla *chat*, sennò l'altra cosa che possiamo fare è aprire un foglio *Excel* e lo condividiamo. Se andaste a questo indirizzo dovreste poter accedere a questo foglio *Excel*. Vi chiediamo di mettere qua la vostra chiave pubblica. Ecco, questa è la mia. Ora è arrivato qualcun altro. Quando è avvenuto questo trasferimento è successo letteralmente quello che vi raccontavo nella prima ora, cioè c'è una grande tabella in cui, in corrispondenza della mia chiave pubblica, c'era una certa disponibilità, dopo la mia transazione questa disponibilità è diminuita di una unità ed è aumentata di una unità la disponibilità invece alla riga di Vincenzo. La tabella che rappresenta chi ha che cosa è mutata in questo senso: quella tabella là è il riferimento assoluto che dice chi ha che cosa. Questo poi non ha una controparte fisica di qualche tipo. E senza controparte fisica, perché questa cosa ha valore? Qua potremmo fare un'altra intera giornata. Quello che abbiamo visto è la rappresentazione di quello che vediamo noi tramite il nostro *Wallet*. Ora faremo un po' di scambi e poi andremo a vedere quella famosa lista di transazioni dove tutte le transazioni sono registrate. In quelle trascrizioni vedremo esattamente queste informazioni: da, a, e poi la firma.

Prof. Vincenzo Rana: Questa è semplicemente una tabella in cui abbiamo appuntato i nostri indirizzi come i nostri IBAN. Avremmo potuto scambiarceli via *Whatsapp*, via messaggio, tramite un foglio di carta; quindi, stiamo usando una tabella *Excel* solo perché è molto comoda essendo a distanza. Ora noi prendiamo uno di questi *address*, che non so a chi si riferisce, tra l'altro; quindi, io so che probabilmente è uno di noi perché abbiamo comunicato la tabella, però non so chi. Non c'è modo di risalire a chi è questa persona.

Prof. Francesco Bruschi: Ecco, vedete Vincenzo clicca invia, guardate cosa succede. Si apre questa finestra. Lui indica l'indirizzo del ricevente e poi specifica molto semplicemente la somma. Vedete che cosa viene chiesto: questa è una finestra di ricapitolazione in cui viene chiesta conferma della volontà di mandare 0,2 *Ether* a questo indirizzo. Noi confermiamo. A questo punto il *Wallet* firma con la nostra chiave privata, genera la transazione e la manda alla rete. Adesso questo assegno è stato mandato nella rete, stiamo aspettando che i validatori, cioè quell'insieme di soggetti che sono incentivati a fare questo lavoro, prendano la transazione di Vincenzo e la registrino.

Partecipante al Seminario: Confermo che è arrivata la transazione ma pongo una domanda: qui siamo in un'area di test ovviamente, ma volendo

caricare soldi veri con la carta di credito, quello è un momento tracciabile per le forze di polizia, perché devo comunque fare riferimento a un'identità bancaria precisa.

Prof. Francesco Bruschi: Assolutamente. Quel pagamento avviene con carta di credito, tutti i soggetti che offrono questo servizio in Italia sono soggetti poi a loro volta soggetti agli obblighi *KYC* di identificazione della controparte. Quindi, se lo facessimo su *Coinbase*, prima il sito ci chiederà la carta d'identità, farà un po' di domande, insomma, dovrà adempiere ai suoi obblighi di *KYC*.

Dott. Fabio Di Vizio: Ecco però, per sfruttare questa indicazione: tutti gli scambi che poi avvengono all'interno, prima di uscire, questi in realtà rimangono in un mondo pienamente virtuale, nella piattaforma dell'*Exchange*. Quindi fintanto che lei non farà un prelievo e uscirà, non tornerà in *blockchain*.

Prof. Francesco Bruschi: Esatto. Saranno tutte scritture contabili interne all'*Exchange*.

Dott. Fabio Di Vizio: E quindi scusi, avendo il dato di chi è entrato e poi uscito, per arrivare a collegare i due mondi come momenti unitari di un'unica operazione come si fa? Abbiamo speranza, non dobbiamo arrenderci. Sappiamo però che è complicato.

Prof. Francesco Bruschi: Ora noi lo faremo, lo faremo qui. Proviamo a farlo.

Prof. Vincenzo Rana: Solo un appunto, ovviamente nel *KYC* potrei fare un lavoro, fare qualcosa per cui ricevo questo pagamento, oppure incontro una persona, le do 50 € in contanti e lui manda la criptovaluta. Qua è un po' più difficile perché il *KYC* non c'è. Mentre gli attori sono abilitati a fare questo tipo di cambiavalute, ci sono altre situazioni che sono un po' più particolari.

Prof. Francesco Bruschi: Oppure faccio il *miner*. Se faccio il *miner* mi compro un *computer*, lo attacco alla presa della corrente, lo attacco alla rete. Tramite il *mining* abbiamo capito che posso guadagnarmi degli *Ether* o dei *Bitcoin* che sono creati in modo da non avere nessuna precedente proprietario identificabile: è la rete che lo assegna ad un'identità completamente crittografica. Quindi questo configura un meccanismo di potenziale riciclaggio. Posso tirarmi fuori dei *Bitcoin* completamente nuovi di zecca, non riconducibili a nessuna precedente identità. Qui quello che abbiamo fatto è mandare degli *Ether* a qualcuno di voi. L'invito è che chi li ha ricevuti provi a sua volta a mandarlo a qualche collega.

Prof. Vincenzo Rana: In particolare noi abbiamo mandato a 0X3C67 0,2 *Ether*. Chiederemmo a questo *address*, a questa entità, di mandarne la

metà quindi 0,1 al successivo.

Prof. Francesco Bruschi: Provate anche voi a fare un trasferimento, vedete che cosa comporta e lo farete in modo arbitrario e del tutto libero.

Dott. Fabio Di Vizio: Ingegner Bruschi, prima che scada il tempo dedicato alla nostra sessione, le chiedo di trattare qualche tema compatibile con il tempo residuo.

Prof. Francesco Bruschi: Sì, certamente. A questo punto abbiamo avuto l'idea di come sia facile scambiarsi, ricevere e trasferire gli *asset*. A questo punto, però andiamo a esplorare quella questione che dicevamo prima: per quello che ho detto, tutte queste transazioni devono essere documentate e accessibili, come in effetti sono. Quindi andiamo a guardare dentro la *blockchain*: ci baseremo su un servizio offerto da una società collegata alla *Blockchain* che ci consente di guardare dentro la *blockchain*. Questo è del tutto analogo a quanto ha fatto prima il vostro collega: è andato su *blockchain*. *com*. Questi servizi sono servizi che chiunque può utilizzare per curiosare il contenuto della *blockchain*. Questo è un sito (*Etherscan*) che ci dà accesso, ci consente di sbirciare dentro la *blockchain*. Qui, per esempio, noi possiamo andare a farci gli affari dell'*address* di Vincenzo. Ora Vincenzo metterà il suo *address*, ma chiunque di noi potrebbe mettere l'*address* di Vincenzo. Vediamo che questa è la storia dell'indirizzo che Vincenzo ha creato, qua abbiamo la storia delle transazioni che interessano Vincenzo. Ciascuna di queste transazioni è la transazione di Vincenzo. Se andiamo a cliccare su *transaction hash*, ognuna di queste è proprio quelle informazioni che dicevamo: da chi parte, per esempio, questa è la transazione con la quale io l'ho finanziato; Vedete? Questo qui è il mio indirizzo. A chi e quanto qui non viene rappresentata, ma possiamo andarlo a recuperare, c'è anche la firma crittografica. Quindi se volessimo, potremmo autonomamente verificare che questa transazione è valida e corretta. Quindi vedete che guardando l'indirizzo di Vincenzo si vede che qualcuno gli ha mandato un *Ether*; chi è questo? Clicca sul mio indirizzo e vede che sono io. Queste sono tutte le transazioni che mi riguardano, quindi vedete che io sono un soggetto attivo. Spero che il vostro istinto investigativo non venga sollecitato da questa circostanza: in realtà questo è l'indirizzo che uso per fare dimostrazioni.

Partecipante al Seminario: Quindi è come vedere l'estratto conto di una banca, di un conto corrente. Dare-avere.

Prof. Francesco Bruschi: Esattamente.

Prof. Vincenzo Rana: Qui è addirittura collegato, quindi posso cliccare sul destinatario e andare a vedere il conto del destinatario, vedere che transazione ha fatto, cliccare ancora, andare avanti nell'analisi: quindi ho tutto lo

storico di tutte le transazioni.

Prof. Francesco Bruschi: E quindi qui si possono vedere tutti i soggetti coi quali ho avuto dei rapporti economici.

Prof. Vincenzo Rana: Proviamo a vedere un percorso: questo è l'*address* di Francesco: 16 minuti fa ha fatto un versamento di un *Ether* a un indirizzo che noi sappiamo essere il mio, però vediamo un indirizzo. Io clicco sull'indirizzo e vediamo che questo indirizzo non ha mai operato prima: la prima operazione l'ha fatta 17 minuti addietro; quindi, potrei immaginare che sia stato neo-creato. Non ne ho la prova, però è abbastanza evidente. Questo non è stato utilizzato giorni o mesi fa e la prima cosa che fa è ricevere un *Ether* da questo indirizzo e poi fa due operazioni: trasferisce 0,2 a qualcuno e 0,2 a qualcun altro. Vediamo la prima transazione, quella che ho fatto circa 9/10 minuti fa. Io l'ho data a questo indirizzo, clicco sull'indirizzo ed ecco che vediamo questo indirizzo. Ha ricevuto 0,2 *Ether* 9 minuti fa e quattro minuti fa ne ha dati 0,1 a un altro indirizzo ancora. Andiamo a questo indirizzo ancora e vediamo che questo indirizzo l'unica cosa che ha fatto è ricevere 5 minuti fa 0,1 *Ether* senza nessuna operazione e abbiamo seguito il percorso da Francesco fino a dove questi 0,1 *Ether* si sono fermati. Rimangono gli altri 0, 9 che sono invece sparpagliati: in parte li ho io, in parte li hanno gli altri *address*.

Prof. Francesco Bruschi: Quindi, come vedete, tutto è completamente visibile a chiunque. Queste analisi le abbiamo fatte noi, le potete fare voi, le può fare chiunque altro. Una precisazione relativa alla domanda che è stata fatta precedentemente: "*Ma se ad un certo punto Etherscan, che è un servizio offerto dalla società, chiude, io non posso più guardare la blockchain?*" In realtà posso farlo, la *blockchain* è sempre accessibile, semplicemente questo è un servizio offerto che è conveniente perché ha un'interfaccia molto potente; quindi, se io dovessi accedere direttamente alla *blockchain*, otterrei dei dati che sono più grezzi quindi dovrei organizzarli. Ma tutta l'informazione sarebbe comunque accessibile.

Dott. Fabio Di Vizio: Prima di avviarci a conclusione, il collega Ruta voleva fare una domanda.

Dott. Gaetano Ruta: Vedendo quest'ultimo prospetto che lei ha mostrato, mi viene abbastanza spontanea una domanda: questo, che è un equivalente di un estratto conto, con tutte le movimentazioni in ordine cronologico, è in chiaro oppure no? Quello che io non capisco, questo *Etherscan*, che dovrebbe essere l'equivalente della denominazione di un istituto bancario, è un soggetto al quale si possono indirizzare, lo dico in maniera un po' *naif*, un ordine di esibizione per capire che cosa c'è dietro queste transazioni finanzia-

rie? E quei codici alfanumerici che sono indicati per esprimere la posizione e del beneficiario e del disponente, possono essere in chiaro oppure no? Nella prospettiva del magistrato inquirente sembra saltare tutta la logica antiriciclaggio, cioè non facciamo altro che aggiornare le normative antiriciclaggio di anno in anno sulla base delle direttive dell'Unione europea e poi abbiamo canali per i quali alla fine rischiamo di poter verificare soltanto il momento di entrata e di uscita, ma non tutto quello che succede nel mezzo.

Prof. Vincenzo Rana: Per rispondere, voglio far vedere una cosa. Noi siamo su un sito ma possiamo andare su un altro sito, per esempio *Blockscout* col mio indirizzo e vedete esattamente le stesse informazioni. Cioè sono interfacce, e ce ne possono essere diverse e questi sistemi non sono responsabili dei dati, semplicemente li mostrano.

Prof. Francesco Bruschi: Esatto, queste sono solo delle interfacce che prendono dei dati che sono pubblicamente accessibili a chiunque. Non è che lo siano per difetto di protezione. Lo so, questo carattere pubblico è assolutamente connaturato, essenziale a questi mezzi, cioè questi mezzi si basano sul fatto che queste informazioni siano pubbliche il più possibile. Quindi *Etherscan* è semplicemente un intermediario che non può in nessun modo agire attivamente, per esempio inibendo il trasferimento, può soltanto rappresentare con un'interfaccia conveniente e potente i dati. Quindi se io dico a *Etherscan* "*ora tu questo indirizzo mi dici chi è*", lui alza le mani e ci dice "*guarda, io ne so esattamente quanto te. Ti posso rappresentare questa stringa che è una chiave pubblica*".

Dott. Fabio Di Vizio: Non potremmo neanche dire che è pubblica: dà accesso alla lettura, tutto qua. Non possiamo neanche dire che stia pubblicando il dato, perché in realtà dà accesso alla lettura di un dato pubblico. Però il collega prima chiedeva, lui non ha avuto modo di vederlo: le prime schede, quelle dove c'è Paolo Rossi, Pippo e la stringa alfanumerica. Lui vuole andare da Paolo Rossi, che tutto sommato pensa che sia qualcuno che ha una strada, una casa e una vita riconoscibile, qualcosa su cui fare un'adeguata verifica, che tutto sommato corrisponde. Come passiamo dalla stringa a Paolo Rossi?

Prof. Francesco Bruschi: Qui la stringa non ha un'automatica e immediata corrispondenza con un'identità anagrafica, con un soggetto individuabile. Quello che noi possiamo fare è lavorare induttivamente, quindi ci chiediamo: chi è questo che controlla questa chiave? E come facciamo a farlo? Abbiamo diversi meccanismi. Uno è: vediamo con chi ha interagito, quindi non so chi è lui, ma so che ha preso dei soldi da quest'altro indirizzo, quest'altro indirizzo sono in grado di identificarlo? Magari no. Vado avanti così, a ritroso, fino a quando posso imbattermi in un indirizzo che già cono-

sco per altre ragioni oppure mi imbatto in una transazione che origina da un soggetto che è tenuto per esempio all'identificazione dei propri utenti, come dicevamo prima.

Dott. Fabio Di Vizio: Dunque, per così dire, siamo alla ricerca di un momento di compromissione; rispetto alla possibilità di continuare a lavorare sul *blockchain* senza dichiararsi vi sono però momenti in cui l'*Exchange* è tenuto alla verifica, così come un *Custodian Wallet Provider*. In ogni caso la ricerca è per approssimazione e ragionamento induttivo. Questo vi dimostra, torno alla tematica della configurabilità del riciclaggio sotto il profilo dell'ostacolo all'identificazione della provenienza delittuosa delle somme, quanto si resti ostacolati nel momento in cui delle disponibilità passano da un indirizzo a un altro: ci possiamo arrivare, ma la difficoltà è consistente.

Prof. Francesco Bruschi: Vorrei specificare che adesso vi stiamo rappresentando questo lavoro di induzione a mano, perché ovviamente così lo si capisce. Esistono strumenti che lo automatizzano. Quindi immaginate, volendo identificare un indirizzo, un *software* che automaticamente insegue tutte queste tracce, potenzialmente le triangola. Quindi, per esempio, potrei scoprire che questo indirizzo che sto attenzionando ha lo stesso insieme di soggetti con i quali interagisce un altro indirizzo, di cui però per qualche ragione conosco l'identità e dunque, forse, tra i due soggetti c'è qualche affinità. Quindi posso utilizzare queste cose che posso estrarre utilizzando un *software* che è in grado di seguire migliaia di queste tracce in un modo impraticabile per chi dovesse farlo manualmente.

Dott. Fabio Di Vizio: Professori, a questo punto devo necessariamente chiudere la sessione perché la puntualità è qualità apprezzata non meno dei contenuti. Devo ringraziarvi, di cuore. Per il contributo di conoscenza che avete offerto, destando molto interesse rispetto a un tema che, tutto sommato, nel tempo a disposizione, potevamo trattare nelle componenti istituzionali e che invece è stato esaminato lungamente, per rispondere all'esigenza di necessaria competenza che la materia presuppone. Credo che sia ben emersa la consapevolezza, come dicevo in apertura, che alcuni miti, per esempio quello di una completa disintermediazione, forse per fortuna, sono solo tali e alcune realtà, invece, ibride, collegate, interconnesse, sono quelle con cui siamo chiamati realmente a confrontarci. Ringrazio molto tutti coloro che hanno seguito con tanto interesse i lavori di questa intensa mattinata.

Prof. Francesco Bruschi: Grazie per le domande che testimoniano un'attenzione vivace, una grande competenza e un grande intuito.

Bibliografia essenziale

Bruschi F. - Paulon T. - Rana V. - Sciuto D., *A privacy preserving identification protocol for smart contracts*, ISCC 2021: 1-6

Bruschi F. - Paulon T. - Rana V. - Sciuto D., *A Protocol for On-Chain Tenders*, PerCom Workshops 2022: 273-278

Bruschi F. - Rana V. - Pagani A. - Sciuto D., *Acknowledging Value of Personal Information: a Privacy Aware Data Market for Health and Social Research*, DLT@ITASEC 2020

Bruschi F. - Rana V. - Pagani A. - Sciuto D., *Tunneling Trust Into the Blockchain: A Merkle Based Proof System for Structured Documents*, IEEE Access 9: 103758-103771 (2021)

Bruschi F. - Tumiati M. - Rana V. - Bianchi M. - Sciuto D., *A Decentralized System for Fair Token Distribution and Seamless Users Onboarding*, ISCC 2020: 1-6

Bruschi F., *Le applicazioni delle nuove tecnologie: Criptovalute, Blockchain e Smart Contract*, in *Il diritto industriale*, volume 2/2020, pp. 162-164

Cortesi E. - Bruschi F. - Secci S. - Taktak S., *A new approach for Bitcoin pool-hopping detection*, Comput. Networks 205: 108758 (2022)

Di Vizio F., *Gli obblighi antiriciclaggio per operatori in valute virtuali*, in *Discrimen*, 2 dicembre 2019

Di Vizio F., *Il decreto legislativo 125/19 e l'attuazione della quinta direttiva europea antiriciclaggio*, in *Foro italiano*, anno CXLV, n. 2, febbraio 2020, parte V, col. 66-73

Di Vizio F., *Le cinte daziarie del diritto penale alla prova delle valute virtuali degli internauti, Lo statuto delle valute virtuali: le discipline e i controlli*, in *Diritto penale contemporaneo*, 2 ottobre 2018, fascicolo 10/2018, p. 21-81 e in *Fintech, Regole e Mercati*, Napoli, 291 e ss.

Di Vizio F., *Lo statuto penale delle valute virtuali: le discipline e i controlli*, in *Discrimen*, 19 giugno 2019

Di Vizio F., *Moderni abusivismi e criptovalute. Tra il mito della completa disintermediazione e la realtà di nuovi intermediari*, in *Discrimen*, 22 aprile 2022

I reati ambientali e gli illeciti in tema di circolazione dei rifiuti. Presentazione degli interventi

di Pasquale Fimiani*

Nella individuazione dei reati ambientali il riferimento di base è rappresentato dalla direttiva 19 novembre 2008, n. 2008/99/CE[1], la quale prevede[2] un elenco analitico di illeciti per i quali gli Stati membri devono apprestare la tutela penale[3].

L'ambito delineato dalla direttiva n. 2008/99/CE – in questo confermato dalla definizione di danno ambientale dettata dall'art. 300 del d.lgs. n. 152/2006 (di seguito anche T.U.A.) in conformità a quella prevista dalla direttiva 2004/35/CE[4] – esclude dal suo spettro applicativo la materia del paesaggio e riguarda i fenomeni nei quali risulta compromessa o messa in pericolo la salubrità ambientale, nel duplice profilo di aggressione a *specifiche componenti naturalistiche* meritevoli di tutela (specie ed habitat naturali protetti, ovvero aree naturali protette) ovvero agli elementi fondamentali delle acque e del suolo.

Tenendo però presente "la nozione complessa e plurivoca di paesaggio", la quale, secondo la recente giurisprudenza[5], "non è più riconducibile al solo ambiente naturale statico, ma è concepibile quale frutto dell'interazione tra uomo e ambiente che, valorizzando anche gli aspetti identitari e culturali, si fonda sulla sintesi dell'azione di fattori naturali, umani e delle loro interrelazioni"[6], la materia va inclusa in una accezione ampia di ambiente ed ascritta, per la sua peculiarità e le tecniche di tutela, al versante della protezione integrale.

In questo contesto generale vanno individuati i reati ambientali il cui accertamento può essere agevolato dall'uso dell'intelligenza artificiale.

(*) Avvocato generale della Corte di Cassazione, componente del Comitato Scientifico FVO.

1) Direttiva del Parlamento europeo e del Consiglio sulla tutela penale dell'ambiente, recepita con il d.lgs. n. 121/2011 ed ulteriormente attuata con la legge n. 68/2015 recante l'introduzione dei delitti ambientali nel codice penale.
2) Peraltro, dettando norme minime, per cui «gli Stati membri hanno facoltà di mantenere in vigore o adottare misure più stringenti finalizzate ad un'efficace tutela penale dell'ambiente», purché "compatibili con il Trattato" (Considerando n. 12).
3) In data 15 dicembre 2021 la Commissione europea ha presentato la nuova proposta di direttiva sostitutiva della direttiva n. 2008/99/CE, la quale conferma l'elenco degli illeciti con alcune integrazioni.
4) Direttiva Parlamento europeo e del Consiglio del 21 aprile 2004 sulla responsabilità ambientale in materia di prevenzione e riparazione del danno ambientale.
5) Cons. Stato, sez. IV, n. 624/2022.
6) Di "*interazione tra elementi ambientali ed antropici che caratterizza il paesaggio*" parla anche Cass. pen., sez. III, n. 370/2020.

Un primo aspetto riguarda il rapporto tra reati ambientali e criminalità organizzata, considerato che in questa materia la Procura nazionale antimafia ed antiterrorismo dispone di una avanzata banca dati che potrebbe fornire, incrociata con quelle specifiche in materia ambientale, utili indicazioni investigative.

Il tema sarà affrontato dal collega Ardituro.

Sono stati poi selezionate due tipologie di reati strettamente connesse tra loro, legate alle tematiche della circolazione dei rifiuti e della contaminazione e bonifica dei siti, affidate, rispettivamente ai colleghi Galanti ed Affinito.

Al fine di introdurre tali relazioni, va precisato che dall'art. 259, comma 2, T.U.A. (per il quale: «alla sentenza di condanna, o a quella emessa ai sensi dell'art. 444 del c.p.p., per i reati relativi al traffico illecito di cui al comma 1 o al trasporto illecito di cui agli articoli 256 e 258, comma 4, consegue obbligatoriamente la confisca del mezzo di trasporto») si evincono due nozioni distinte: il traffico e il trasporto illecito di rifiuti.

Il reato di traffico illecito è previsto dall'art. 259, comma 1, T.U.A. e riguarda la spedizione di rifiuti transfrontaliera in contrasto con la disciplina eurounitaria.

Il trasporto illecito di rifiuti, a sua volta, comprende più fattispecie e precisamente l'esecuzione di trasporto di rifiuti:

– in assenza di iscrizione;

– con carenza dei requisiti e delle condizioni richiesti dalle iscrizioni o comunicazioni (punita, rispettivamente, dall'art. 256, commi 1 e 4)[7];

– con violazione delle regole per la tenuta del formulario di cui all'art. 193 (prevista come reato dall'art. 258, comma 4, prima parte, se riguarda rifiuti pericolosi).

Completa il quadro il reato di attività organizzate per il traffico illecito di rifiuti.

Rientrano inoltre negli illeciti in tema di circolazione dei rifiuti i reati di falso nella certificazione analitica (art. 258, comma 4, seconda parte).

Tali falsi, come emerge dalla prassi, sono finalizzati a simulare l'abusivo smaltimento sotto l'apparente liceità di un'operazione diversa, scopo che viene perseguito:

– classificando falsamente i rifiuti;

– ricorrendo alla pratica del cosiddetto «giro bolla»;

7) Cass. pen., sez. III, n. 12865/2003 ha precisato che «è sanzionato penalmente il trasporto di rifiuti senza autorizzazione e, pertanto, ai fini della punibilità del fatto, non è richiesto lo scarico degli stessi in qualche luogo».

– utilizzando falsi certificati di smaltimento per simulare lo sversamento o l'abbandono illecito dei rifiuti.

Comune a tali tipologie di illecito è, di regola[8], la declassificazione dei rifiuti, la cui natura viene modificata tramite la falsificazione della documentazione di accompagnamento (certificati di analisi, formulari), all'origine presso i produttori o lungo il tragitto presso centri intermedi di stoccaggio. In tal modo i rifiuti vengono compresi sotto codici che presuppongono costi di gestione notevolmente inferiori rispetto a quelli dovuti.

La verifica di tali illeciti può compiersi in primo luogo verificando la falsità dei certificati di analisi o partendo dalla disponibilità dei rifiuti (es. in seguito a sequestro del mezzo che li trasporta), ovvero compiendo una verifica *ex post* della documentazione concernente attività già compiute e che si presume falsa sulla base di elementi indiziari (ad esempio dopo il sequestro del mezzo e l'analisi dei rifiuti trasportati, si accerta la falsità della documentazione di accompagnamento e si passa alla verifica a ritroso delle operazioni compiute nel passato).

In entrambi i casi la verifica va concentrata sul contenuto del certificato e sulla struttura del laboratorio che lo ha confezionato.

Ulteriori verifiche possono farsi nel caso in cui alla declassificazione si accompagni il cosiddetto «giro bolla» (o se si preferisce «triangolazione»). Trattasi di operazione in forza della quale i rifiuti sono cartolarmente fatti transitare da uno stoccaggio all'altro (di regola di più regioni), con il fine della declassificazione della tipologia, per aggirare, in particolare, le normative imperative di carattere generale e regionale, e/o per ovviare alle prescrizioni autorizzative dell'impianto al quale il rifiuto è destinato (che, ad esempio, è autorizzato per lo smaltimento di specifiche categorie di rifiuti ovvero che è abilitato al solo recupero). Si tratta, in sostanza, di trasformare documentalmente la disciplina giuridica del rifiuto in modo da renderla compatibile con la destinazione finale prescelta.

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 e, in alcuni casi senza miscelazione con altri rifiuti, è inviato per lo smaltimento/recupero finale. Considerata la tecnica seguita il passaggio

8) Anche se la simulazione dell'avvenuto smaltimento può prescindere dalla declassificazione dei rifiuti, ciò è quello che nella prassi avviene. Sarebbe incongruo (ed antieconomico), invero, che i rifiuti prima vengano correttamente qualificati e poi, anziché giungere agli impianti di trattamento ordinari, siano smaltiti abusivamente (mediante abbandono, interramento, sversamento nella pubblica fognatura, in mare, ecc).

intermedio è assolutamente necessario.

La prova di tale movimento può ricavarsi dal riscontro tra le annotazioni poste sul registro di carico e scarico dei rifiuti e le bolle di accompagnamento in uscita dal centro di stoccaggio. qualora il quantitativo dei rifiuti presi in carico e quello dei rifiuti in uscita corrisponde, ovvero vi sia una estrema vicinanza tra l'orario di arrivo e quello di ripartenza, è evidente che i rifiuti hanno subito il trasbordo diretto, poiché se i medesimi fossero stati effettivamente scaricati, trattati e successivamente ricaricati non vi potrebbe essere tale corrispondenza.

L'esame del cronotachigrafo e dei documenti di viaggio dei mezzi utilizzati, l'acquisizione delle risultanze delle operazioni di pesatura dei mezzi in entrata ed uscita dagli impianti, l'assunzione di testimonianze dei dipendenti del centro di stoccaggio, il prelievo, a sorpresa, di campioni presso depositi, vasche e simili esistenti presso quest'ultimo, possono consentire di acquisire elementi a conferma della inesistenza del passaggio intermedio dei rifiuti (a tali verifiche può ricorrersi anche nel caso di simulazione dell'avvenuto smaltimento/recupero dei rifiuti).

L'applicazione di tali profili indiziari è stata riconosciuta dalla S.C.: «L'esistenza di una irregolare tenuta dei registri obbligatori di carico e scarico, di sistematiche attività di miscelazione di rifiuti pericolosi tra loro e di rifiuti pericolosi con altri non pericolosi, l'effettuazione di miscelazioni in assenza di accertamenti tecnici preliminari e in assenza dei necessari trattamenti preliminari, il mancato rispetto delle cautele necessarie rispetto alla gestione di rifiuti pericolosi, l'apposizione del codice CER privilegiando la compatibilità con le autorizzazioni dei destinatari e la compatibilità con le esigenze commerciali rispetto alla effettiva composizione dei materiali inviati, la conseguente destinazione di rifiuti in prevalenza pericolosi a impianti che non avrebbero potuto riceverli, la modifica di codice CER, e non solo il mero giro bolla, rispetto a rifiuti non sottoposti ad alcun trattamento costituiscono condotte che valutate nel loro insieme con riferimento, ovviamente, al singolo impianto, denotano manifesta illiceità, e ciò a prescindere dal fatto che l'impianto potesse, quale produttore non originario indicare se stesso come produttore dei rifiuti e dal fatto che in condizioni di rispetto delle altre formalità e cautele il c.d. giro bolla possa non rivestire carattere di intrinseca illiceità. Ciò che rileva è che la mancata indicazione della provenienza iniziale dei rifiuti nei formulari e il ricorso al giro bolla costituiscono metodologia scelta ed utilizzata all'interno di un meccanismo che muove dalla irregolare tenuta dei registri di carico-scarico e termina con la destinazione ad altri impianti di prodotti diversi per caratteristiche rispetto a quanto dichiarato, frutto

di miscelazioni non operate nei limiti e con le garanzie previste e, infine, marcati con codici CER non fedeli alle caratteristiche prevalenti della miscela e apposti avendo riguardo alle opportunità commerciali»[9].

Altra linea investigativa praticabile è quella di verificare i movimenti finanziari tra i soggetti che compiono le operazioni descritte. Queste presentano l'apparenza di una operazione lecita conclusa a costi in realtà superiori a quelli reali. Si pone quindi l'esigenza di redistribuire quanto in più solo formalmente dovuto. Di qui il ricorso a false fatturazioni che il produttore, o soggetto a lui collegato, emette nei confronti dello smaltitore/recuperatore finale per operazioni inesistenti (spesso per generiche «consulenze ambientali»), al fine di compensare la pregressa ed inversa fatturazione per operazioni di smaltimento in realtà non effettuate.

L'esame di questi temi è propedeutico all'approfondimento del tema dell'uso della tecnologia nell'accertamento e prevenzione dei reati ambientali, per il quale si rinvia alle relazioni del Tenente Colonnello Corsano e del prof. Giuseppe Sgorbati.

9) Cass. pen., sez. III, n. 47870/2011.

Le banche dati nazionali in materia ambientale

di Luca Meoli*

1. Premessa

Si indicano di seguito le banche dati nazionali in materia ambientale[1].

1.1. SISPED

Il Ministero dell'ambiente e della sicurezza energetica, in linea con quanto previsto dai Regolamenti UE nn. 1013/2006 e 660/2014, ha istituito un sistema informatico 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.

1.2. 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.

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.

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

(*) Colonnello della Guardia di Finanza.

1) Per le fonti da cui trarre informazioni sulle banche dati che seguono, si rinvia al *Position Paper* presentato dalla Fondazione Occorsio in Roma, il 19 novembre 2021, in *fondazioneoccorsio.it*.

1.3. M.U.D.

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 dichiarazioni presentate dai soggetti obbligati sono raccolte dalle Camere di Commercio, che procedono alla loro informatizzazione 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.

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

1.4. Catasto rifiuti ISPRA

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, 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.

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

1.5. Osservatorio rifiuti sovraregionale (O.R.SO.)

O.R.SO. è un'applicazione *web-based*, utilizzata in 16 Regioni, 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.

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.

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 O.R.SO., per quanto riguarda le Regioni aderenti, sono utilizzati da ISPRA per la compilazione delle pertinenti informazioni del Catasto Nazionale dei Rifiuti.

1.6. Catasto georeferenziato impianti rifiuti (C.G.R. Web)

Il C.G.R. Web è un *database* condiviso da Regione e Province lombarde, che è stato istituito nella prospettiva di disporre di un unico archivio informatizzato in cui sono presenti i dati tecnici, amministrativi e geografici relativi agli:

– 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;

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

– 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).

All'interno del Catasto, consultabile liberamente, è inoltre disponibile l'applicativo "*Viewer Criteri Localizzativi*", il quale consente di accedere alla cartografia relativa alle aree idonee e non idonee alla localizzazione degli impianti di trattamento dei rifiuti.

Il programma di sviluppo del C.G.R. prevede nel tempo di trasferire in unico *database* regionale i contenuti delle diverse banche dati utilizzate dalle

singole Autorità competenti.

Sono attualmente disponibili i dati relativi a inceneritori e discariche in esercizio.

Per completezza, si citano, da ultimo, le banche dati fiscali 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 modalità di accesso/utilizzo e trattamento (titolarità) delle informazioni ivi contenute, ancorché effettuate avvalendosi di un sistema di intelligenza artificiale.

Tre ambiti in cui la tecnologia può essere di supporto nel contrasto ai reati ambientali

di Antonello Ardituro*

1. Criminalità organizzata ed ambiente

"*Dotto', a' munnezza è oro!*". Con questa colorita espressione, un collaboratore di giustizia, riferendosi a fatti di fine anni '80, con un sorriso beffardo, iniziava la sua narrazione ai magistrati napoletani sulle potenzialità economiche dell'affare rifiuti per la criminalità organizzata.

Quella affermazione, all'epoca considerata folcloristica e suggestiva, si è rivelata, con il trascorrere degli anni ed il susseguirsi delle indagini, particolarmente veritiera e capace di dipingere con poche parole un quadro di inquietante commistione fra criminalità organizzata, imprenditoria, politica, malaffare.

Indagini complesse nel settore sono state compiute dalla Direzioni Distrettuali Antimafia del meridione, ma il "caso napoletano" o meglio campano, appare quello maggiormente in grado di rappresentare un paradigma per affrontare le diverse angolazioni del tema proposto.

Infatti, è in Campania che si è assistito, prima e più che in altri luoghi, all'occupazione da parte delle organizzazioni criminali mafioso-camorristiche di interi settori dell'economia, sia nella gestione del ciclo legale dei rifiuti, sia nello smaltimento illecito dei rifiuti speciali e pericolosi.

Deve infatti considerarsi che le organizzazioni criminali nella consapevolezza, acquisita molto prima di quanto abbiano fatto le istituzioni legali dello Stato, che la "*munenzza è oro*", hanno investito sia nel ciclo legale che in quello illegale dello smaltimento dei rifiuti, attraverso accordi corruttivi con pezzi delle istituzioni e dell'imprenditoria nazionale, ed acquisendo nel tempo professionalità in tutti i settori di smaltimento dei rifiuti: solidi urbani, speciali, tossici e pericolosi. Si è accertato che la camorra ha investito in ogni settore del traffico di rifiuti, presentandosi pronta a fronteggiare ogni esigenza del mercato, legale e illegale, come una grande agenzia di fornitura di servizi ed in particolare: La raccolta, lo stoccaggio e lo smaltimento dei rifiuti industriali, dei rifiuti speciali e dei rifiuti tossici e nocivi; la gestione illegale di discariche abusive per lo smaltimento di rifiuti di diverso genere,

(*) Sostituto Procuratore nazionale antimafia ed antiterrorismo.

compreso quelli solidi urbani; il controllo del sistema degli appalti pubblici per la raccolta dei rifiuti, per la costruzione delle discariche, e degli impianti speciali di smaltimento; la predisposizione delle imprese "mafiose" necessarie a risolvere le situazioni di emergenza, per la raccolta, il trasporto e lo smaltimento; l'offerta delle professionalità utili per la bonifica di zone devastate dalle discariche abusive; l'attività illegale di estrazione di materiale da cave o specchi di acqua e la successiva riutilizzazione di tali zone con lo sversamento illegale di rifiuti, così facendo sistema con l'altro grande affare legato al ciclo del calcestruzzo.

Di converso, miopia politica e affarismo clientelare hanno caratterizzato l'arretramento degli enti territoriali di fronte al problema smaltimento, con la creazione di una voragine coperta dalla diretta partecipazione della camorra a tali attività economiche.

Dunque, deve innanzitutto sfatarsi la diffusa convinzione che quando nel settore dei rifiuti si parla di ingerenze e di interessi della criminalità organizzata, si sta trattando esclusivamente degli sversamenti illeciti in discariche non autorizzate. La mafia e la camorra con i rifiuti hanno sempre da guadagnare e, se sono certamente in grado di garantire gli sversamenti illeciti, con costi evidentemente concorrenziali rispetto alle procedure legali (in particolare per rifiuti speciali e pericolosi), esse hanno anche acquisito, per mezzo di *imprese-mafiose* professionalità e disponibilità di mezzi, per infiltrare il ciclo legale dei rifiuti.

Nel settore degli sversamenti illeciti sono stati monitorati i trasporti di tonnellate di rifiuti speciali e tossici provenienti per lo più dalle imprese industriali del Centro Nord e destinati ad improvvisate discariche della provincia di Napoli e di Caserta. Il territorio cambiava, vecchie cave venivano riempite, e nuove collinette spuntavano, colme di rifiuti e di fusti coperti da terreno ed erbacce[1]. Con conseguenti falde acquifere contaminate e prodotti della terra avvelenati. In un sistema in cui tutti hanno ricavato un guadagno: l'imprenditore industriale perché riusciva a smaltire a prezzi dimezzati, con tanto di documentazione certificante lo smaltimento; l'imprenditore del trasporto, perché si garantiva inimmaginabili volumi d'affari; il camorrista, perché rica-

1) Con conseguente demitizzazione del tradizionale codice d'onore propalato per decenni dalla stessa criminalità organizzata, che si è costantemente vantata del consenso fondato sulla teoria della "difesa del propria gente e del proprio territorio". Le indagini hanno dimostrato in maniera univoca che il clan dei casalesi, per formulare l'esempio più rilevante, formalmente legato alla sua purezza mafiosa, non ha esitato a farsi artefice, mosso da intenti esclusivamente di speculazione e profitto economico, di uno dei più gravi disastri ambientali del nostro Paese, avvelenando i terreni dell'agro aversano, riversando rifiuti speciali e pericolosi di provenienza industriale, smaltendo fanghi tossici capaci di inquinare le falde acquifere di una terra fertilissima e fonte di prodotti di altissima qualità, come la mozzarella di bufala, il pomodoro sammarzano e la albicocca pellecchiella.

va una fonte irripetibile di guadagno costante (i rifiuti "non finiscono" mai), lontana dagli ordinari controlli delle forze dell'ordine, generalmente impegnate a reprimere i reati a base violenta del clan (estorsioni e fatti di sangue)[2].

Nel settore del ciclo legale dei rifiuti, la criminalità organizzata ha infiltrato le procedure di aggiudicazione degli appalti, con imprese ad essa collegate o del tutto controllate dai clan[3]. Come si vedrà, nel tempo il sistema di infiltrazione mafiosa nel ciclo dei rifiuti, si è avvalso di diverse modalità operative, tutte finalizzate a medesimo obiettivo, ma sempre più raffinate. Dallo schema classico dell'impresa amica "imposta" nelle procedure di aggiudicazione o, preferibilmente, nell'affidamento dei subappalti, si è passati alla tecnica del "tavolino" a tre gambe (il politico o funzionario sua espressione, l'imprenditore, il camorrista) quale luogo parallelo e prevalente di determinazione delle scelte dell'ente pubblico; fino a giungere all'impresa mafiosa che oggi appare in grado, grazie alle notevoli disponibilità economiche ed al know-how acquisito di gareggiare e vincere le gare in tutta autonomia, da oligopolista del settore che non teme il confronto con gli altri competitori economici ed imprenditoriali.

L'impresa mafiosa, ormai di terza generazione, ha allontanato completamente da sé, il legame visibile con la sua provenienza criminale ed opera sul mercato forte della sua autonoma capacità imprenditoriale.

Intendiamoci: l'emergenza e la crisi sono sempre benvenute, in qualsiasi settore di intervento, per la criminalità organizzata, poiché esse sono sintomo di disorganizzazione, di mancanza di regole, di provvedimenti straordinari da adottare, di necessità imprenditoriali da assolvere in poco tempo, tutte condizioni in cui chi esercita il controllo del territorio, e dispone di immense

2) In altre parole, se l'ingresso della camorra nel settore dei rifiuti è determinato dalla ricerca di profitti illeciti, l'incontro con l'impresa avviene perché quell'offerta incontra una corrispondente domanda di servizi illegali, tali da ridurre i costi e, quindi, massimizzare i profitti. L'impresa chiede un servizio alla camorra e la camorra offre tale servizio: essa si fa carico della domanda delle imprese italiane di scaricare sulla collettività e sulle generazioni future il peso economico di una corretta gestione del ciclo dei rifiuti.

3) Nell'ambito di indagini condotte dalle Direzioni Distrettuali Antimafia, si è puntualmente constatato, per esempio che nella documentazione contabile di noti esponenti mafiosi, sequestrata nell'ambito di attività di diversa natura, si rinvenivano documenti da cui emergeva l'incidenza della tangente tratta dal servizio di raccolta degli Rsu. Si rilevava da singole investigazioni poi, con significativa regolarità, l'assunzione sistematica di familiari di esponenti di clan camorristici nelle società affidatarie dei servizi; noli, da parte degli enti pubblici, di veicoli di proprietà di persone legate ad affiliati; l'acquisizione della gestione di siti – uso discarica o stoccaggio provvisorio – nella titolarità di persone vicine ai clan. Si accertava la sorprendente identità soggettiva – nel tempo – degli intermediari operanti sul mercato dei rifiuti, già arrestati o indagati, per le relazioni con le organizzazioni mafiose. Si tratta di un quadro talmente pregno di concordanti evidenze indiziarie da poter essere agevolmente sostenuta la tesi che vede nel controllo del ciclo gestionale dei rifiuti uno degli scopi tipici del programma delle organizzazioni mafiose, evidentemente per la sua particolare redditività.

liquidità economiche e finanziarie, tanto da proporsi come "*l'unica soluzione al problema*", di fronte alle incapacità politiche, agli appetiti della burocrazia, ed alle necessità delle imprese produttive.

La camorra risolve i problemi: ha la possibilità di procurare i terreni, di mettere a disposizione i mezzi per il trasporto veloce; garantisce che la popolazione non reagisca alla localizzazione dei siti.

La crisi poi, come puntualmente avvenuto in Campania, richiama interventi emergenziali dal punto di vista istituzionale ed economico: di qui il Commissariato per l'emergenza rifiuti ed un fiume di denaro di volta in volta, per più di venti anni, riversato nella disponibilità di funzionari a volte corrotti e spesso incapaci[4]. Soldi da impiegare nei consorzi, nel nolo dei mezzi, nella

4) Appartiene ormai al notorio giudiziario (e non solo) la critica situazione del ciclo gestorio dei rifiuti in Campania che ha provocato lo stato di emergenza, a partire dal 1994, data in cui avvenne la nomina del primo Commissario di Governo. Le cause principali alla base della cronica situazione emergenziale sono state individuate da specifiche indagini, evincendosi una assoluta carenza di pianificazione, incapacità – nella migliore delle ipotesi – nell'individuazione di attrezzate discariche, inadeguatezza degli impianti di trattamento dei rifiuti nei sette impianti di produzione di C.D.R. (combustibile derivato dai rifiuti), nei ritardi nella realizzazione dei termovalorizzatori, negli ostacoli posti da parte della popolazioni di alcuni territori e da parte anche della camorra, nei livelli inaccettabili di raccolta differenziata. Dal 1994 ad oggi, "l'emergenza" ha costituito comunque la norma e ne è seguito, quale risultato, la stagnazione dei rifiuti per le strade od in improvvisati siti di stoccaggio provvisorio trasformati, di fatto, in discariche abusive, il tutto con il coinvolgimento degli operatori istituzionali che si ponevano di fatto *contra legem*.
Nessun dubbio che, in tale situazione, risultava naturale l'inserimento dei professionisti, "broker" del settore, di rado estranei agli interessi mafiosi. La percezione dei rischi igienico-sanitari da parte delle popolazioni locali, seppur tardiva e collegata ai soli fenomeni più eclatanti (ossia la mancata raccolta del rifiuto dal "cassonetto"), alimentava progressivamente il disagio sociali. Tale disagio era tale da trasmodare talora – deve ritenersi per ignoranza – nel rogo dei cumuli di rifiuti, con amplificazione del pericolo sanitario, atteso il rischio di emissioni di diossina.
L'emergenza dei rifiuti a Napoli e nella sua regione inizia convenzionalmente l'11 febbraio del 1994, con l'istituzione del primo decreto del Presidente del Consiglio dei Ministri, pubblicato sulla Gazzetta Ufficiale n. 35 del giorno successivo. Il Governo prendeva così atto dell'emergenza ambientale venutasi a creare nelle settimane precedenti in numerosi centri campani, a causa della saturazione di alcune discariche. Si individuava, per questa ragione, nel Prefetto di Napoli, l'organo di Governo in grado di sostituirsi a livello territoriale a tutti gli altri enti territoriali coinvolti a vario titolo e preposto quindi a gestire i poteri commissariali straordinari. Tra il 1994 ed il 1996 la gestione dell'emergenza rifiuti passò attraverso l'ampliamento della capacità di versamento grazie alla requisizione di diverse discariche private in tutta la regione, poi date in gestione all'Ente per le Nuove Tecnologie, l'Energia e l'Ambiente. Nel marzo 1996 il Governo interveniva nuovamente nella gestione commissariale del Prefetto individuando la figura commissariale nella persona del Presidente della Regione: al Prefetto rimaneva la gestione del servizio di raccolta, al Presidente della Regionale veniva affidato il compito di redazione del Piano Regionale e per gli interventi urgenti in tema di smaltimento. Nel giugno 1997 era pubblicato il Piano Regionale per lo smaltimento dei rifiuti che prevedeva la realizzazione di due termovalorizzatori e sette impianti per la produzione di combustibile derivato dai rifiuti. Nel luglio 1998 un'apposita commissione parlamentare constata la permanenza della situazione emergenziale, giudicava insufficienti gli impianti realizzati o individuati e poco collaborative le amministrazioni locali. Nel dicembre 2000, secondo il Prefetto di Napoli, le discariche esistenti sarebbero risultate ormai tutte saturate, il che – unitamente alla mancata individuazione degli impianti di produzione di combustibile derivato dai rifiuti – riproduceva la situazione preesistente. All'inizio del 2001 si registrava una

costruzione delle discariche, tutti settori nei quali la concorrenza fra gli imprenditori interessati è stata spiazzata dall'intervento criminale delle imprese della camorra.

L'emergenza attiva i meccanismi di infiltrazione e di gestione illecita sia nel ciclo legale che nel ciclo illegale; si tratta di un meccanismo normativo (dichiarazione dello stato di emergenza e superamento della normativa appalti) e fattuale (necessità di intervenire subito per esigenze sanitarie ed ambientali), in una delle zone più inurbate d'Europa.

Il caso Campania, poi, si è caratterizzato anche per una assolutamente originale legislazione dell'emergenza, che ha inciso addirittura sulle norme di diritto penale, sostanziale e processuale, con interventi normativi speciali ed eccezionali, di discutibile compatibilità costituzionale, quali quelli del d.l. 90 del 2008 (conv. in l. 123/08), che istituiva temporaneamente la Procura della Repubblica regionale in materia di rifiuti, e quello del d.l. 6 novembre 2008, conv. in l. 210/2008 che introduceva nuove fattispecie sanzionatorie vigenti solo nei territori in cui vige lo stato di emergenza.

2. I delitti in materia ambientale e il doppio binario

Questo il quadro di riferimento entro il quale approfondire la riflessione in matria di rifiuti, prendendo spunto dalle esperienze più rilevanti degli ultimi decenni.

Con l'ulteriore osservazione che, come noto, l'attività di indagine ha scontato per lungo tempo l'assenza di specifici strumenti normativi di contrasto.

È mancato, infatti, fino al 2001, un delitto che sanzionasse le condotte principali; l'inquadramento del caso giudiziario nel delitto associativo si pre-

---

nuova pesante crisi risolta solo attraverso la riapertura provvisoria delle discariche di Serre e Castelvolturno e l'invio di circa mille tonnellate al giorno di rifiuti verso altre regioni, quali la Toscana, l'Umbria e l'Emilia Romagna, nonché all'estero, in Germania. Nei due anni successivi entravano in funzione gli impianti di produzione di combustibile derivato a Caivano, Avellino e Santa Maria Capua Vetere (alla fine del 2001), in seguito a Giugliano, a Casalduni e a Tufino (nel 2002), infine a Battipaglia nel 2003. Gli impianti risulteranno peraltro colpevolmente inefficienti. I sette impianti che avrebbero dovuto produrre il combustibile da rifiuto producevano dunque milioni di eco balle, insuscettibili di "termovalorizzazione", rimanendo giacenti in siti di stoccaggio provvisorio trasformati in discariche spesso abusive. Anche la frazione umida prodotta dagli impianti non risultava nelle specifiche, dovendo dunque essere ugualmente trattata quel rifiuto. In tale contesto si inseriva – come tradizione – la criminalità organizzata, unica in grado di mediare tra le collettività locali e le istituzioni, così garantendosi cospicui profitti a fronte dell'utilizzo di società o terreni riferibili ad esponenti del gruppo.

L'emergenza aveva il suo punto più alto a partire dai primi giorni del 2008, quando dal Commissariato si manifestava la volontà di riaprire la mega discarica di Pianura. Sono noti a tutti i disordini e le devastazioni che ne scaturirono e che sono state monitorate anche dal punto di vista investigativo e giudiziario.

sentava particolarmente difficile anche perché i possibili reati-fine di natura ambientale avevano natura di contravvenzioni, residuando solo le ipotesi, assai difficili da provare, di falso e corruzione. Le capacità tecniche più adeguate si rinvenivano nelle sezioni specializzate delle Procure Circondariali che, di converso, erano però ostacolate dalla cronica mancanza di mezzi, da sempre riservati alla Procure presso il Tribunale, ed essendo in *nuce* minata ogni possibilità di coordinamento sul territorio nazionale. Le competenze alle indagini preliminari nelle Procure presso il Tribunale erano frammentata fra le sezioni assegnatarie dei delitti contro la pubblica amministrazione, ovvero suddivise – a pioggia – tra le diverse sezioni; ed anche quando l'indagine sorgeva direttamente in capo alla Direzione Distrettuale Antimafia, per effetto delle dichiarazioni dei collaboratori di giustizia, essa era condotta da magistrati per un verso privi delle competenze specialistiche per altro orientati generalmente a sottovalutare l'importanza dell'indagine stessa, a fronte di notizie di reato o delazioni collaborative in altri settori criminali. Infine, scarse sono sempre state le risorse di polizia giudiziaria nel settore dei rifiuti, ed assai ridotte quelle specialistiche, quali i servizi del Nucleo Operativo Ecologico dei Carabinieri.

È a partire dall'unificazione degli Uffici di Procura – gennaio 2000 – che è stato più facile coniugare la professionalità dei magistrati esperti nelle indagini di criminalità organizzata e de in possesso, anche per la consultazione della Banca dati, di conoscenze sull'attività delle imprese mafiose ben oltre i territori di influenza dei singoli clan, con la specializzazione dei magistrati esperti in materia ambientale, con conseguente aumento della capacità di risposta al complesso fenomeno.

E grazie all'entrata in vigore del primo delitto ambientale, l'art. 53-*bis* del d.lgs. n. 22/97, che è stato introdotto dalla legge 23.03.2001, n. 93, poi riproposto nell'art. 260 d.lgs. 152/06, ed oggi previsto dopo la riserva di codice dall'art. 452-*quaterdecies*, che sanziona il traffico illecito di rifiuti in forma organizzata, si è realizzata una effettiva svolta normativa e nel contrasto investigativo, che ha consentito di indagare sui rapporti fra criminalità organizzata e violazione della normativa ambientale e sui rifiuti.

Si tratta di una norma che sanziona condotte non necessariamente legate al contesto associativo, ma che quando opera in tali ambiti, consente, in quanto delitto, di procedere con le regole del doppio binario, anche grazie alla possibilità di contestare l'aggravante mafiosa, nonché di consideralo delitto fine del reato di cui all'art. 416-*bis* c.p., nell'ambito di programma criminoso che può comprendere i delitti di corruzione, turbativa d'asta, false fatturazioni, falso in certificazioni, intestazione fittizia di beni e società.

Connotazioni caratteristiche soprattutto in ordine alla possibilità di avvalersi del regime speciale in materia di intercettazioni, e con riferimento al termine di prescrizione del reato, non solo perché, in una materia da sempre considerata di scarso rilievo dal legislatore, che si è limitato a prevedere norme contravvenzionali di contrasto, si è introdotta una ipotesi delittuosa, ma anche perché la possibile concorrente aggravante mafiosa, induce all'applicazione di termini di prescrizione molto più lunghi.

Del resto, sulla base della giurisprudenza di legittimità, una norma come quella del traffico organizzato di rifiuti codifica un delitto che va considerato di per sé "di criminalità organizzata", secondo un insegnamento che ormai risale al 2005, allorquando le Sezioni Unite[5], pronunciandosi in tema di applicabilità dell'art. 240-*bis*, comma secondo, disp. coord. cod. proc. pen. dettarono le coordinate per una corretta definizione di reato di criminalità organizzata, facendo riferimento oltre che ai delitti di criminalità mafiosa elencati dall'art. 51 co. 3-*bis* c.p.p., anche all'associazione per delinquere (art. 416 c.p.), ed alle fattispecie associative previste da norme incriminatrici speciali, nonché ai delitti ad essi connessi ed a quelli a partecipazione plurisoggettiva caratterizzati da un apparato organizzato stabile.

Individuato dunque nell'"organizzazione" il carattere fondamentale per individuare le fattispecie appartenenti al *genus* "criminalità organizzata", non può che apparire immediatamente riferibile a tale categoria il delitto di traffico organizzato di rifiuti, a prescindere dal suo realizzarsi in contesti che consentono l'applicazione dell'aggravante mafiosa, con le conseguenti applicazioni normative legate al doppio binario (per es. in materia di intercettazioni).

Fin dalla introduzione dell'art. 53-*bis* d.lgs. 22/97, la Corte di Cassazione, nell'ambito di una puntuale verifica ermeneutica, ne aveva individuato gli elementi caratterizzanti fra cui: l'autore del reato può essere "chiunque", in quanto la pluralità di agenti non è richiesta come elemento costitutivo della fattispecie; si tratta di una fattispecie monosoggettiva e non di concorso necessario, anche se nella pratica può assumere di fatto carattere associativo e di criminalità organizzata; l'elemento soggettivo richiesto dalla norma è il dolo specifico, ossia il fine di conseguire un ingiusto profitto (ricavi o risparmi nei costi); l'elemento oggettivo consiste in una attività di gestione dei rifiuti "organizzata", con allestimento dei mezzi necessari, ossia in una attività "imprenditoriale"; l'attività di gestione mira al traffico illecito, come si ricava dal titolo della norma, e può riguardare una o più delle diverse fasi in cui si concreta ordinariamente la gestione dei rifiuti nella fase dinamica (cessione; rice-

5) Cass. pen., sez. un., 11 maggio 2005, n. 17706.

zione, trasporto, esportazione e importazione), sia interna, che internazionale (le condotte non sono tassative come emerge dall'avverbio "comunque"); l'attività di gestione deve essere caratterizzata non dalla episodicità, ma da una "pluralità di operazioni" e dalla "continuità" in senso temporale: il "traffico illecito" ha senso se è caratterizzato da più operazioni e se presenta un elemento temporale adeguato; il quantitativo di rifiuti deve essere "ingente": l'interprete dovrà valutare caso per caso questo requisito, traendo elementi di comparazione anche dalle previsioni di reati contravvenzionali in tema di rifiuti; l'attività di gestione deve essere "abusiva" (mancanza di autorizzazioni, iscrizioni o comunicazioni previste dalla normativa od anche autorizzazioni scadute o palesemente illegittime) con riferimento ad attività organizzata clandestina od anche apparentemente legittime; l'offensività della condotta non riguarda necessariamente la messa in pericolo della incolumità pubblica ma certamente attiene – sia pure non ontologicamente ed in modo indiretto – al bene giuridico dell'ambiente. Precisa la Suprema Corte che "*il traffico illecito di rifiuti, anche quando organizzato ed abituale, con ingenti quantità di rifiuti, ordinariamente produce un reale pericolo per l'ambiente o di fatto un danno ambientale, tuttavia, si ripete, il reato sussiste quando ne ricorrono i presupposti formali e non è di per se un reato di danno o di pericolo concreto, pur dovendo questi aspetti essere valutati dal giudice quali conseguenze eventuali del reato*" (Cass. Sez. III nr. 1446 del 16.12.2005).

Proprio in relazione al danno, deve evidenziarsi come la giurisprudenza abbia più volte precisato le caratteristiche del danno ambientale che è una conseguenza quasi fisiologica del traffico organizzato di rifiuti. In particolare, la Suprema Corte ne ha evidenziato la triplice dimensione: personale, quale lesione del fondamentale diritto all'ambiente salubre da parte di ogni individuo; sociale, quale lesione del diritto all'ambiente nelle articolazioni sociali nelle quali si sviluppa la personalità umana; pubblica, quale lesione del diritto-dovere pubblico spettante alle Istituzioni centrali e periferiche. In concreto è evidente che il danno provocato dalla violazione della normativa ambientale si realizza attraverso l'inquinamento dei terreni, la contaminazione delle falde acquifere, l'alterazione della flora e delle coltivazioni, la modifica finanche della linea paesaggistica, con conseguente affiancamento dell'emergenza alimentare a quella ambientale. In questo modo, il danno ambientale diviene dunque disastro ambientale, con diretta incidenza sulla salute delle persone e con il danneggiamento irreversibile di luoghi e di cose. Si tratta, come noto, di fatto che nel tempo la giurisprudenza ha faticosamente sussunto nell'art. 434 c.p., in mancanza di una norma espressa, poi introdotta con l'art. 452-*quater* c.p.; il disastro innominato si caratterizzava per la capacità di tutela della "messa in pericolo" del

bene "incolumità pubblica", indipendentemente dal verificarsi in concreto del danno, il quale però si prefigurato come verosimile per effetto di condotte che mettono a rischio l'incolumità di un numero indefinito di persone. Dunque, un reato di pericolo presunto, rientrante nella categoria dei reati di pura condotta, ovvero di quelli per i quali si prescinde dalla causazione di un evento, in cui il legislatore anticipa al massimo il momento della punibilità della condotta, in considerazione della estrema rilevanza dei beni tutelati.

La specifica fattispecie di cui all'art. 452-*quater* ha invece espressamente indicato cosa si intenda per disastro ambientale, facendo riferimento a: l'alterazione irreversibile dell'equilibrio di un ecosistema; l'alterazione dell'equilibrio di un ecosistema la cui eliminazione risulti particolarmente onerosa e conseguibile solo con provvedimenti eccezionali; l'offesa alla pubblica incolumità in ragione della rilevanza del fatto per l'estensione della compromissione o dei suoi effetti lesivi ovvero per il numero delle persone offese o esposte a pericolo. La fattispecie valorizza gli elementi del vecchio art. 434 c.p., ma si distingue in quanto con la nuova fattispecie può configurarsi disastro ambientale anche senza messa in pericolo della pubblica incolumità, e viceversa.

3. Banche dati e intelligenza artificiale. Il ruolo propulsivo della Direzione nazionale antimafia e antiterrorismo

Il compendio normativo di diritto sostanziale a cui si è fatto riferimento e la connotazione del traffico organizzato di rifiuti quale delitto di criminalità organizzata, non necessariamente mafiosa, ha indotto ad attrare la materia ambientale nell'ambito di interesse della Direzione nazionale antimafia ed antiterrorismo che, ormai da anni, si propone come soggetto privilegiato di monitoraggio e di impulso di attività investigative, grazie alla possibilità di catalogare ed analizzare le informazioni provenienti dalle Procure territoriali nell'ambito della banca dati Sidda-Sidna. La natura, ormai chiara, transregionale o transnazionale del traffico illecito di rifiuti, la partecipazione alle attività illecite di soggetti di diversa provenienza criminale, politica, imprenditoriale, la partecipazione di broker specializzati e gli accordi fra clan mafiosi di distinta origine territoriale, la necessità di superare la dimensione circondariale delle strutture organizzative giudiziarie ed investigative, impongono un ruolo attivo della Procura nazionale. Invero pur in mancanza di una norma di legge, la Procura nazionale, ha opportunamente sollecitato l'inserimento in Banca Dati di atti relativi ad indagini in materia ambientale di particolare rilievo e comunque di quelli attinenti al traffico organizzato di rifiuti, nonché la segnalazione da parte dele Procure non operanti a livello distrettuale,

di indagini di interesse ultra-territoriale, attraverso la catalogazione dei cd. reati spia di condotte a potenzialità mafiosa.

Monitoraggio e catalogazione di informazioni, analisi delle condotte e dei fenomeni, richiedono l'attuazione di nuove modalità di indagine e di adeguati sistemi di prevenzione che, oggi, non possono non richiamare all'applicazione al settore dell'intelligenza artificiale.

Assolutamente indispensabile appare, per esempio, operare per una corretta gestione del *data mining*, in quanto il settore è caratterizzato dalla esistenza di una gran quantità di informazioni organizzate in banche dati di diversa natura, pubblica, privata, scientifica, giudiziaria, che non dialogano fra loro e non condividono le informazioni. Una prima applicazione di sistemi di intelligenza artificiale andrebbe compiuta in questo ambito assolutamente prioritario e farebbe compiere di per sé un salto di qualità alle attività di prevenzione e di indagine.

Lo studio approfondito del territorio, la verifica attenta di luoghi di smaltimento e/o di combustione dei rifiuti, la classificazione della loro natura e delle specifiche caratteristiche, la presenza di determinati siti di produzione economica e industriale, ove oggetto di preciso monitoraggio e raccolta dati, consentirebbe, mediante appositi algoritmi, di operare mediante prototipi di alta efficienza ed efficacia, in un settore che rappresenta, almeno negli intendimenti, la priorità di intervento delle più importanti Agenzie internazionali, degli Stati dell'occidente e del nostro stesso Paese, che ne ha fatto una delle linee fondamentali del Piano Nazionale di Ripresa e Resilienza, nell'ambito di un progetto pluriennale di interventi per la transizione ecologica.

L'organizzazione di traffico illecito di rifiuti

di Alberto Galanti*

1. Introduzione

La tematica della tutela dell'ambiente ha avuto negli ultimi anni un crescente interesse nell'opinione pubblica e nella comunità internazionale.

Prova ne sia, per quanto concerne l'Italia, la recente introduzione nella costituzione italiana di un esplicito riferimento all'ambiente, operato mediante la modifica dell'articolo o della Costituzione, nonché l'espressa indicazione della prevalente del diritto ad un ambiente salubre rispetto al concorrente (sovente antagonista) diritto alla libertà di iniziativa economica privata, operato con la modifica all'articolo 41.

A livello sovranazionale, inoltre, la pressante emergenza costituita dai cambiamenti climatici ha indotto la Corte EDU a ritenere ammissibile il ricorso presentato da Duarte Agostinho et al. c/Portogallo + 32, in cui i ricorrenti (sei giovani portoghesi) hanno denunciato che 33 Stati firmatari del Trattato di Parigi del 2015 (tra cui l'Italia) sarebbero venuti meno al loro obbligo di limitare il cambiamento climatico tramite la riduzione delle emissioni di gas serra, così violando gli articoli 2, 8 e 14 della CEDU, così ponendo in pericolo la vita, la salute e la vita familiare delle generazioni a venire.

In tale clima di rinnovato slancio ambientalista si inserisce la legge 68/2015, la quale ha introdotto un intero titolo del codice penale rubricato "dei delitti contro l'ambiente", in cui è confluito anche il delitto già previsto dall'art. 51-*bis* del d.lgs. 22/1997 (c.d. "decreto Ronchi") e poi dall'articolo 260 del d.lgs. 152/2006 (c.d. "Testo Unico Ambientale" o "TUA"), quello relativo alla "attività organizzata per il traffico illecito dei rifiuti", che dei delitti contro l'ambiente rappresenta il capostipite e l'archetipo.

L'espunzione della norma penale dal TUA non è senza conseguenze. Ed infatti, nella struttura della norma vi è l'esplicito riferimento ad elementi costitutivi del reato che rimandano alle definizioni e alla disciplina contenuta nel Testo Unico: dalla nozione di "rifiuto", a quella di "gestione", fino alla "abusività" della condotta, è evidente che l'interprete non può fare a meno di riferirsi, pur in assenza di una disposizione formalmente non strutturata come una "norma penale in bianco", agli istituti disciplinati dal decreto 152/2006.

(*) Sostituto Procuratore D.D.A. di Roma.

2. L'esclusione dalla Parte IV del Testo Unico Ambientale

Il primo punto da tenere a mente è lo stesso ambito di applicazione della normativa sui rifiuti.

Il decreto, infatti, disciplina (art. 1) le seguenti materie:

a) nella parte seconda, le procedure per la valutazione ambientale strategica (VAS), per la valutazione d'impatto ambientale (VIA) e per l'autorizzazione ambientale integrata (IPPC);

b) nella parte terza, la difesa del suolo e la lotta alla desertificazione, la tutela delle acque dall'inquinamento e la gestione delle risorse idriche;

c) nella parte quarta, la gestione dei rifiuti e la bonifica dei siti contaminati;

d) nella parte quinta, la tutela dell'aria e la riduzione delle emissioni in atmosfera;

e) nella parte sesta, la tutela risarcitoria contro i danni all'ambiente.

Tutto ciò che è estraneo alla Parte Quarta del decreto è pertanto estraneo alla disciplina dei rifiuti e, a cascata, al precetto penale in argomento. A tal proposito, l'articolo 185 del decreto 152/2006 stabilisce che sono escluse dal campo di applicazione della parte quarta del decreto:

a) le emissioni costituite da effluenti gassosi emessi nell'atmosfera di cui all'articolo 183, comma 1, lettera z);

b) gli scarichi idrici, esclusi i rifiuti liquidi costituiti da acque reflue;

c) i rifiuti radioattivi;

d) i rifiuti risultanti dalla prospezione, dall'estrazione, dal trattamento, dall'ammasso di risorse minerali o dallo sfruttamento delle cave;

e) le carogne ed i seguenti rifiuti agricoli: materie fecali ed altre sostanze naturali non pericolose utilizzate nelle attività agricole ed in particolare i materiali litoidi o vegetali e le terre da coltivazione, anche sotto forma di fanghi, provenienti dalla pulizia e dal lavaggio dei prodotti vegetali riutilizzati nelle normali pratiche agricole e di conduzione dei fondi rustici, anche dopo trattamento in impianti aziendali ed interaziendali agricoli che riducano i carichi inquinanti e potenzialmente patogeni dei materiali di partenza;

f) le eccedenze derivanti dalle preparazioni nelle cucine di qualsiasi tipo di cibi solidi, cotti e crudi, non entrati nel circuito distributivo di somministrazione, destinati alle strutture di ricovero di animali di affezione di cui alla legge 14 agosto 1991, n. 281, nel rispetto della vigente normativa;

g) i materiali esplosivi in disuso;

h) i materiali vegetali non contaminati da inquinanti provenienti da alvei di scolo ed irrigui, utilizzabili tal quale come prodotto, in misura superiore

ai limiti stabiliti con decreto del Ministro dell'Ambiente e della Tutela del Territorio da emanarsi entro novanta giorni dall'entrata in vigore della parte quarta del presente decreto. Sino all'emanazione del predetto decreto continuano ad applicarsi i limiti di cui al decreto del Ministro dell'Ambiente 25 ottobre 1999, n. 471;

i) il coke da petrolio utilizzato come combustibile per uso produttivo;

l) materiale litoide estratto da corsi d'acqua, bacini idrici ed alvei, a seguito di manutenzione disposta dalle autorità competenti;

m) i sistemi d'arma, i mezzi, i materiali e le infrastrutture direttamente destinati alla difesa militare ed alla sicurezza nazionale individuati con decreto del Ministro della Difesa, nonché la gestione dei materiali e dei rifiuti e la bonifica dei siti ove vengono immagazzinati i citati materiali, che rimangono disciplinati dalle speciali norme di settore nel rispetto dei principi di tutela dell'ambiente previsti dalla parte quarta del presente decreto. I magazzini, i depositi e i siti di stoccaggio nei quali vengono custoditi i medesimi materiali e rifiuti costituiscono opere destinate alla difesa militare non soggette alle autorizzazioni e nulla osta previsti dalla parte quarta del presente decreto;

n) i materiali e le infrastrutture non ricompresi nel decreto ministeriale di cui alla lettera m), finché non è emanato il provvedimento di dichiarazione di rifiuto ai sensi del decreto del Presidente della Repubblica 5 giugno 1976, n. 1076, recante il regolamento per l'amministrazione e la contabilità degli organismi dell'esercito, della marina e dell'aeronautica[1].

Tra le varie esclusioni dianzi evidenziate, particolarmente rilevante è la distinzione tra "scarichi" e "rifiuti liquidi".

La nozione di "scarico" (e non più "acque di scarico" come nella previgente disciplina), è fornita dall'art. articolo 74 del TUA, che lo definisce come "qualsiasi immissione effettuata esclusivamente tramite un sistema stabile di collettamento che collega senza soluzione di continuità il ciclo di produzione del refluo con il corpo ricettore in acque superficiali, sul suolo, nel sottosuolo e in rete fognaria, indipendentemente dalla loro natura inquinante, anche sottoposte a preventivo trattamento di depurazione". Confermando una consolidata giurisprudenza, Cassazione, Sezione 3^, sentenza 14 febbraio 2018, n. 6998 (in proc. Martiniello), ha ribadito che «lo scarico è tale in quanto avvenga tramite condotta, tubazioni, o altro sistema stabile di collettamento, intendendosi, per condotta, non per forza tubazioni o altre

1) Ai sensi del comma 2 dell'art. 185, per quanto concerne i sottoprodotti di origine animale non destinati al consumo umano si applica la disciplina di cui al regolamento (CE) n. 1774/2002 del Parlamento europeo e del Consiglio del 3 ottobre 2002, che costituisce disciplina esaustiva ed autonoma nell'ambito del campo di applicazione ivi indicato.

specifiche attrezzature, essendo, invece, necessario e sufficiente un sistema di deflusso, oggettivo e duraturo, che comunque canalizza, senza soluzione di continuità, in modo artificiale o meno, i reflui fino al corpo ricettore. In tutti gli altri casi – nei quali manchi il nesso funzionale e diretto delle acque reflue con il corpo recettore – si applicherà, invece, la disciplina sui rifiuti, di cui alla Parte IV del d.lgs. 152/2006».

Ciò che distingue pertanto un rifiuto liquido da uno scarico è l'esistenza o meno di uno "stabile collettamento" tra la sorgente del liquido e la sua destinazione finale.

Tuttavia, come si vedrà in appresso, per il solo percolato di discarica, il problema può essere risolto anche mediante la verifica della sussistenza degli elementi in presenza dei quali una sostanza può essere qualificata come "rifiuto".

Altro caso peculiare è costituito dal materiale terroso scavato e ammassato; in tale ipotesi sarà necessario verificare in concreto se ci si trovi di fronte a materiali risultanti dalla prospezione, dall'estrazione, dal trattamento, dall'ammasso di risorse minerali o dallo sfruttamento delle cave, in sostanza a materiale di cava (escluso dalla disciplina dei rifiuti), oppure a dei "rifiuti", ovvero ancora a delle "terre e rocce da scavo" di cui all'art. 186 TUA (che sono un particolare tipo dei "sottoprodotti" di cui all'art. 184-*bis*): solamente negli ultimi due casi ci si troverà di fronte all'applicazione della normativa sui rifiuti e occorrerà accertare se sarà applicabile la normativa sui rifiuti o quella sui sottoprodotti.

Pertanto, in presenza di un regolare titolo abilitativo alla coltivazione di una miniera o di una cava, il materiale estratto non potrà essere considerato rifiuto, ma materia prima (diverso è il caso, lo si vedrà in appresso, di attività autorizzata da un titolo illegittimo).

3. L'esclusione "postuma" dalla qualifica di rifiuto

Una volta verificato di essere nell'ambito di applicazione della Parte Quarta del TUA, va evidenziato che vi sono dei casi in cui, in presenza di determinate condizioni, un rifiuto cessa di essere tale. Si potrebbe in questo caso parlare di "esclusione postuma" dalla disciplina dei rifiuti, rispetto a quella analizzata in precedenza, che è una esclusione "ontologica"[2].

Il primo caso è quello dell'End of waste (EOW), disciplinato dalla direttiva 2008/98/CE del 19 novembre 2008 (c.d. "direttiva quadro", o *fra-*

2) Così il sottoscritto ne "*I delitti contro l'ambiente - Analisi normativa e prassi giurisprudenziali*", Pacini Giuridica, 2021, pag. 132.

mework directive, in materia di rifiuti) e ribattezzato dal legislatore italiano come "cessazione della qualifica di rifiuto", disciplinato dall'art. 184-*ter* del TUA.

L'EOW ha sostituito la previgente disciplina delle c.d. "materie prime secondarie" (articolo 181-*bis* del TUA) spostando il *focus* della disciplina dal "risultato" di un processo di recupero al processo stesso. L'*End of waste* potrebbe pertanto definirsi come un "processo di recupero del rifiuti", al termine del quale il rifiuto cessa di essere tale e torna a svolgere un ruolo utile nel circuito economico come "prodotto".

Va precisato che il termine EOW indica tutte le fasi del processo che determina il passaggio da un rifiuto a un prodotto: fino al completamento del processo, il rifiuto resta tale (stesso principio vale per i sottoprodotti).

Le condizioni che determinano la possibilità per un rifiuto di cessare di essere tale sono indicate dall'articolo 184-*ter* del TUA, secondo cui un rifiuto cessa di essere tale, quando è stato sottoposto a un'operazione di recupero, incluso il riciclaggio, e soddisfi i criteri specifici, da adottare nel rispetto delle seguenti condizioni:

a) la sostanza o l'oggetto è comunemente utilizzato per scopi specifici;

b) esiste un mercato o una domanda per tale sostanza od oggetto;

c) la sostanza o l'oggetto soddisfa i requisiti tecnici per gli scopi specifici e rispetta la normativa e gli *standard* esistenti applicabili ai prodotti;

d) l'utilizzo della sostanza o dell'oggetto non porterà a impatti complessivi negativi sull'ambiente o sulla salute umana.

La qualifica di EOW può essere assegnata a tipologie di materiali da regolamenti comunitari ovvero dal legislatore nazionale. Si tratta dei c.d. "EOW tipizzati".

La normativa europea ha disciplinato solo alcune ristrette ipotesi di EOW:

– regolamento (UE) n. 333/2011 del 31 marzo 2011 recante "I criteri che determinano quando alcuni tipi di rottami metallici cessano di essere considerati rifiuti ai sensi della direttiva 2008/98/CE del Parlamento Europeo e del Consiglio";

– regolamento (UE) n. 1179/2012 del 10 dicembre 2012 recante "I criteri che determinano quando i rottami di vetro cessano di essere considerati rifiuti ai sensi della direttiva 2008/98/CE del Parlamento europeo e del Consiglio";

– regolamento (UE) n. 715/2013 del 25 luglio 2013 recante "I criteri che determinano quando i rottami di rame cessano di essere considerati rifiuti ai sensi della direttiva 2008/98/CE del Parlamento Europeo e del Consiglio".

L'Italia a sua volta ha disciplinato i seguenti casi di End of Waste:

– decreto del Ministero dell'Ambiente 14 Febbraio 2013, n. 22, "Regolamento recante disciplina della cessazione della qualifica di rifiuto di determinate tipologie di combustibili solidi secondari (CSS), ai sensi dell'articolo 184-*ter*, comma 2, del decreto legislativo 3 aprile 2006, n. 152, e successive modificazioni";

– decreto del Ministero dell'Ambiente 28 marzo 2018, n. 69, "Regolamento recante disciplina della cessazione della qualifica di rifiuto di conglomerato bituminoso ai sensi dell'articolo 184-*ter*, comma 2 del decreto legislativo 3 aprile 2006, n. 152", in vigore dal 3 luglio 2018;

– decreto del Ministero dell'Ambiente 15 maggio 2019 n. 62, "Regolamento recante disciplina della cessazione della qualifica di rifiuto di prodotti assorbenti per la persona (PAP) ai sensi dell'articolo 184-*ter*, comma 2 del decreto legislativo 3 aprile 2006, n. 152";

– decreto del Ministero dell'Ambiente 31 marzo 2020 n. 78, "Regolamento recante disciplina della cessazione della qualifica di rifiuto della gomma vulcanizzata derivante da pneumatici fuori uso, ai sensi dell'articolo 184-*ter*, comma 2 del decreto legislativo 3 aprile 2006, n. 152", in vigore dal 5 agosto 2020;

– decreto del Ministero dell'Ambiente 22 settembre 2020, n. 188, "Regolamento recante disciplina della cessazione della qualifica di rifiuto da carta e cartone, ai sensi dell'articolo 184-*ter*, comma 2, del decreto legislativo 3 aprile 2006, n. 152".

Ai sensi del nuovo paragrafo 4 dell'articolo 6 della direttiva, nel testo modificato dalla direttiva 2018/851/UE, è inoltre possibile, anche ove non sussistano atti normativi relativi a singole sostanze, autorizzare un processo di EOW "caso per caso". Per quanto riguarda l'Italia, il SNPA (servizio nazionale di protezione ambientale) ha emanato le "Linee guida per l'applicazione della disciplina *end of waste* di cui all'articolo 184-*ter*, comma 3-*ter*, del d.lgs. n. 152/2006" (delibera 6 febbraio 2020, n. 62/20), le quali si propongono di "fornire gli elementi utili alla realizzazione di un sistema comune ed omogeneo di pianificazione ed esecuzione delle ispezioni nell'ambito dei processi di recupero o riciclaggio dei rifiuti da cui esitano materiali che hanno cessato di essere rifiuti ai sensi dell'art. 184-*ter*".

Analizzando il documento è possibile distinguere due sottotipi:

– qualora l'autorizzazione faccia riferimento esplicitamente o meno alle norme tecniche individuate dai decreti del Ministro dell'Ambiente 5 febbraio 1998, 12 giugno 2002, n. 161 e 17 novembre 2005, n. 269, che si applicano alle procedure semplificate di recupero dei rifiuti, "possono essere

prese come riferimento tecnico nelle valutazioni istruttorie per il rilascio delle autorizzazioni caso per caso" le disposizioni di cui ai predetti decreti; sono i casi che potremmo definire di End of Waste caso per caso "nominati", ossia già normati dalla disciplina nazionale;

– qualora si tratti di autorizzazioni End of Waste non disciplinate dalla normativa tecnica dianzi menzionata, le Linee Guida prevedono due distinti approcci:

1. se il processo di recupero non rientra tra le casistiche previste dalle norme tecniche dei d.m. 05/02/98 o d.m. 161/02 o DM 269/05, ma esistono comunque degli *standard* tecnici e ambientali riconosciuti (vedi condizione d) della sezione di supporto alle istruttorie), "va fatta una valutazione completa utilizzando le indicazioni previste nella sezione di supporto alle istruttorie";

2. se il processo di recupero non rientra tra le casistiche previste dalle norme tecniche dei d.m. 05/02/98 o d.m. 161/02 o d.m. 269/05 e quindi si tratta di un processo sperimentale in cui definire gli *standard* tecnici e ambientali, la possibilità di utilizzo della materia prima/prodotti in processi o utilizzi su scala reale, va fatta una valutazione completa utilizzando i criteri specifici per la cessazione della qualifica di rifiuti per gli "impianti sperimentali" (ex art. 211 d.lgs. 152/06 e s.m.i.) utilizzando le indicazioni previste nella sezione di supporto alle istruttorie.

Sono quelli che potremmo definire End of Waste caso per caso "innominati".

Sfugge ai tempi del presente contributo un approfondimento in proposito[3], ma a titolo esemplificativo tra i processi EOW autorizzabili, per la sua rilevanza, merita una particolare attenzione il "compost" da rifiuti, che è un fertilizzante e non va confuso con il "composto fuori specifica", che invece è un rifiuto classificato col codice CER 190503.

Altro caso importante è quello dei "fanghi di depurazione", che in presenza di determinate condizioni, si prestano a numerosi utilizzi, ciascuno dei quali può avere una disciplina sua propria:

1. recupero "diretto" mediante spandimento sul terreno;

2. recupero "indiretto" mediante produzione di *compost* (ovvero fertilizzanti e ammendanti, gessi di defecazione, ecc.) da utilizzare in agricoltura;

3. recupero di materie prime dai fanghi (ad esempio il fosforo);

4 trattamento finalizzato alla creazione di nuove materie (ad esempio per la produzione di biodiesel);

5. trattamento termico con recupero di energia.

3) Per un maggiore approfondimento si rinvia a quanto già scritto in A. Galanti, cit., pag. 132 ss.

Il secondo caso è quello dei c.d. "sottoprodotti", disciplinati dall'articolo 184-*bis* TUA ed oggetto di numerosissime modifiche normative.

La norma in via generale stabilisce che perché una sostanza possa qualificarsi come sottoprodotto occorre la concomitante presenza di una serie di requisiti e condizioni, e in particolare:

a. la sostanza o l'oggetto è originato da un processo di produzione, di cui costituisce parte integrante, e il cui scopo primario non è la produzione di tale sostanza od oggetto;

b. è certo che la sostanza o l'oggetto sarà utilizzato, nel corso dello stesso o di un successivo processo di produzione o di utilizzazione, da parte del produttore o di terzi;

c. la sostanza o l'oggetto può essere utilizzato direttamente senza alcun ulteriore trattamento diverso dalla normale pratica industriale;

d. l'ulteriore utilizzo è legale, ossia la sostanza o l'oggetto soddisfa, per l'utilizzo specifico, tutti i requisiti pertinenti riguardanti i prodotti e la protezione della salute e dell'ambiente e non porterà a impatti complessivi negativi sull'ambiente o la salute umana.

Affinché sia utilizzabile la disciplina dei sottoprodotti occorre la compresenza di tutti i requisiti[4].

In entrambi casi evidenziati (EOW e sottoprodotti), trattandosi di una disciplina derogatoria a quella generale sui rifiuti e di particolare favore per il produttore, incombe sul medesimo l'onere della prova della sussistenza di tutti gli elementi in presenza dei quali si verifica la cessazione della qualifica di rifiuto[5].

4. Il delitto di cui all'articolo 452-*quaterdecies* c.p.

L'articolo 452-*quaterdecies* c.p. stabilisce che è punito con la reclusione da uno a sei anni "chiunque, al fine di conseguire un ingiusto profitto,

4) Cass. Pen., Sez. 3^, 4 novembre 2008, n. 47085.

5) Cass. Pen., Sez. 3^, 10 novembre 2016, n. 47262 aveva precisato che il principio dell'inversione dell'onere della prova corrisponde ad un «principio generale già applicato in giurisprudenza: in tema di atti di raggruppamento ed incenerimento di residui vegetali previste dall'art. 182, comma sesto-*bis*, primo e secondo periodo, d.lgs. 152/2006 (cfr. Cass. Pen., sez. III, n. 5504 del 12 gennaio 2016, Lazzarini), di deposito temporaneo di rifiuti (cfr. Cass. Pen., sez. III, n. 29084 del14 maggio 2015, Favazzo), di terre e rocce da scavo (cfr. Cass. Pen., sez. III, n. 16078 del 10 marzo 2015, Fortunato), di interramento in sito della posidonia e delle meduse spiaggiate presenti sulla battigia per via di mareggiate o di altre cause naturali (cfr. Cass. Pen., sez. III, n. 3943 del 17 dicembre 2014, Aloisio), di qualificazione come sottoprodotto di sostanze e materiali (cfr. Cass. Pen., sez. III, n. 3202 del 2 ottobre 2014, Giaccari; sez. III, n. 41836 del 30 settembre 2008, Castellano), di deroga al regime autorizzatorio ordinario per gli impianti di smaltimento e di recupero, prevista dall'art. 258 comma 15 del d.lgs. 152 del 2006 relativamente agli impianti mobili che eseguono la sola riduzione volumetrica e la separazione delle frazioni estranee (cfr. Cass. Pen., sez. III, n. 6107 del 17 gennaio 2014, Minghini), di riutilizzo di materiali provenienti da demolizioni stradali (cfr. Cass. Pen., sez. III, n. 35138 del 18 giugno 2009, Bastone)».

con più operazioni e attraverso l'allestimento di mezzi e attività continuative organizzate, cede, riceve, trasporta, esporta, importa, o comunque gestisce abusivamente ingenti quantitativi di rifiuti".

Nonostante qualche parere contrario in dottrina, il delitto è un reato "comune" che può essere commesso da chiunque e non richiede la qualifica di imprenditore[6]; nonostante la prassi insegni che il delitto in parola viene spesso commesso da soggetti in concorso tra loro, esso è comunque un reato solo "eventualmente plurisoggettivo", ciò che lo distingue in modo chiaro dal reato associativo di cui all'articolo 416. c.p.: l'elemento dell'"organizzazione" non pertiene quindi alla sfera dell'agente di reato bensì a quello dell'attività da esso posta in essere; è un reato di "pericolo astratto" e a consumazione anticipata, che non richiede la compromissione delle matrici ambientali[7]; non è necessariamente correlato a fenomeni di criminalità organizzata[8], anche se spesso, soprattutto in certe aree geografiche, vi si accompagna.

La giurisprudenza, sempre in ordine al soggetto attivo del reato, riconosce la validità della "delega di funzioni"[9], fermo restando l'obbligo, a carico del delegante, di vigilare e di controllare che il delegato usi correttamente la delega[10].

Il reato in parola è inoltre, come emerge dalla definizione ("compimento di più operazioni") ha natura di "reato abituale"[11]: esso sanziona "comportamenti non occasionali" di soggetti che, al fine di conseguire un ingiusto profitto, fanno della illecita gestione dei rifiuti la loro redditizia, anche se non esclusiva, attività, per cui per perfezionare il reato è necessaria una, seppure rudimentale, organizzazione professionale (mezzi e capitali) che sia in grado di gestire ingenti quantitativi di rifiuti in modo continuativo, ossia con pluralità di operazioni condotte in continuità temporale, operazioni che vanno valutate in modo globale: «Alla pluralità delle azioni, che è elemento costitutivo del fatto, corrisponde una unica violazione di legge, e perciò il reato è abituale dal momento che per il suo perfezionamento è necessaria le realizzazione di più comportamenti della stessa specie»[12].

Quanto alla natura "organizzata" dei mezzi e delle attività, la Cassazione ha precisato[13] che «non occorre che tutte le fasi di tale attività vengano

6) Cass. Pen., Sez. 3^, 8 febbraio 2021, n. 4770.
7) Cass. Pen., Sez. 3^, 24 febbraio 2017, n. 9133.
8) Cass. Pen., Sez. 3^, 19 luglio 2017, n. 35568.
9) Vedi, *ex plurimis*, Cass. Pen., 13 dicembre 2011, n. 46819 (in proc. Fioravanti).
10) Cass. Pen., Sez. 3^, 22 aprile 2020, n. 12642.
11) Conforme, *ex plurimis*, Cass. Pen.,13 dicembre 2011, n. 46819 (in proc. Fioravanti).
12) V. anche sez. 3^, 8 luglio 2010, n. 29619 (in proc. Leorati); 15 ottobre 2013, n. 44449 (in proc. Ghidoli); 14 dicembre 2016, n. 52838 (in proc. Camillo e A.).
13) Cass. Pen., Sez. 3^, 28 ottobre 2019, n. 43710.

svolte in forma organizzata e che in ogni fase vi sia la consapevolezza della partecipazione a una attività illecita e il fine di ingiusto profitto, essendo sufficiente, per poter ritenere configurabile il reato, che nell'ambito di detta complessiva attività, si inserisca la condotta di chi, al fine di conseguire un ingiusto profitto, costituisca o si avvalga di una organizzazione allo scopo di realizzare un traffico continuativo e illegale di ingenti quantitativi di rifiuti.

L'attività deve avere ad oggetto "ingenti quantitativi di rifiuti". Quanto al primo aspetto, la Cassazione[14] ha sottolineato come «nel testo della norma non si rinviene alcun dato che autorizzi a relativizzare il concetto, riportandone la determinazione al rapporto tra il quantitativo di rifiuti illecitamente gestiti e l'intero quantitativo di rifiuti trattati nella discarica, per cui l'ingente quantità dev'essere accertata e valutata con riferimento al dato oggettivo della mole dei rifiuti non autorizzati abusivamente gestiti»[15].

Quanto alla nozione di "rifiuto", l'articolo 183 del TUA definisce come rifiuti "le sostanze o gli oggetti che derivano da attività umane o da cicli naturali, di cui il detentore si disfi o abbia deciso o abbia l'obbligo di disfarsi del suddetto materiale". La Cassazione[16] ha chiarito che «la qualifica di rifiuto (art. 183 del d.lgs. 152/2006) deve essere dedotta da dati obiettivi, non dalla scelta personale del detentore che decide che quel bene non gli è più di nessuna utilità. Sono elementi obiettivi, ad esempio, l'oggettività dei materiali in questione, la loro eterogeneità, non rispondente a ragionevoli criteri merceologici, e le condizioni in cui gli stessi sono detenuti, così come le circostanze e le modalità con le quali l'originario produttore se ne era disfatto. Non rileva, poi, il fatto che un bene sia ancora cedibile a titolo oneroso, poiché tale evenienza non esclude comunque la natura di rifiuto».

Quanto all'"obbligo di disfarsi", esso deve derivare da una fonte normativa o da un provvedimento specifico della pubblica amministrazione.

Tornando per un momento al percolato di discarica, va sottolineato come lo stesso ai sensi del decreto legislativo n. 36/2003 "debba" essere raccolto, trattato e, soprattutto, "smaltito" (punto 2.3 dell'Allegato 1). La norma pone quindi in capo al gestore della discarica un vero e proprio "obbligo di disfarsi" del percolato, il che sembra ricondurre in modo chiaro al paradigma dell'articolo 183 del TUA.

L'attività inoltre deve avere ad oggetto la "gestione" di rifiuti. In pro-

14) Cass. Pen., Sez. 3^, 13 luglio 2004, n. 30373.

15) Per quanto concerne il problema della "ingente quantità" la Corte di Cassazione ha affermato la manifesta infondatezza della questione di legittimità costituzionale, sollevata sotto il profilo della indeterminatezza della previsione legislativa, nella sentenza sez. 3^, 12.11.2003, n. 47918.

16) Cass. Pen., Sez. 3^, 24 gennaio 2018, n. 3299.

posito, la Cassazione[17] ha ritenuto che nel concetto di gestione vada inclusa «ogni fase del ciclo dei rifiuti, dal momento della loro produzione alla loro definitiva eliminazione, attraverso l'indicazione delle operazioni che la caratterizzano e che va letta considerando l'insieme delle disposizioni riguardanti la disciplina dei rifiuti e le modalità di svolgimento delle varie operazioni, senza possibilità di scindere e considerare separatamente le singole attività al fine di sottrarle all'applicazione della normativa di settore».

Il requisito che ha creato maggiori difficoltà interpretative è tuttavia quello della "abusività" della condotta.

In proposito si possono effettuare delle distinzioni nella casistica.

Occorre in primo luogo distinguere tra condotta "abusiva" e condotta "clandestina"[18], ossia commessa in totale assenza di autorizzazione.

La "clandestinità" può a sua volta essere "originaria" (mancanza *ab origine* del titolo autorizzativo) ovvero "sopravvenuta" (per scadenza o mancato rinnovo del titolo, ovvero in caso di revoca o annullamento in autotutela del provvedimento).

Alla clandestinità va equiparata la "illiceità" del provvedimento autorizzativo, che concerne il caso in cui esso sia frutto di corruzione o collusione con il funzionario che l'ha rilasciato, nonché la sua "illegittimità"[19].

Altro caso è quello in cui la condotta non sia difforme rispetto alle prescrizioni dell'autorizzazione ma sia contraria a normativa di rango primario o secondario (attività illegale[20]), ovvero a principi di carattere generale che trovano espressione concreta nella normativa tecnica, come nel caso delle c.d. BAT[21] (attività *contra jus*).

Residua poi l'attività svolta in contrasto con le prescrizioni dell'autorizzazione, che potremmo definire attività abusiva "in senso stretto".

---

17) Cass. Pen., Sez. 3^, 7 novembre 2018, n. 50143.

18) Cass. Pen., Sez. 3^, 15 dicembre 2008, n. 46029.

19) V., *ex plurimis*, Cass. Pen., sez. 3^, 7 settembre 2021, n. 33087.

20) Cass. Pen., Sez. 3^, 3 marzo 2010, n. 8299.

21) Le Best Available Tecniques sono elaborate a livello europeo e il loro rispetto costituisce la base per la domanda di AIA e per il suo rilascio o riesame; la loro eventuale sistematica violazione rende "abusiva" l'attività. Analogamente, un'autorizzazione rilasciata in violazione delle BAT di settore, sarà illegittima, rendendo l'attività abusiva (Cass. Pen., Sez. 3^, 7 settembre 2021, n. 33089: «La verifica della rispondenza delle autorizzazioni ambientali alle BAT, in relazione al tipo di attività svolta e alla incidenza della eventuale difformità, e, in ogni caso, il rispetto di queste ultime (anche in questo caso tenendo conto del tipo di attività e della rilevanza della eventuale inosservanza delle BAT Conclusions), assume rilievo al fine dell'accertamento della abusività della condotta, in quanto le stesse concorrono a definire il parametro, di legge o di autorizzazione, di cui è sanzionata la violazione e la cui inosservanza, se incidente sul contenuto, sulle modalità e sugli esiti della attività svolta, può determinare la abusività di quest'ultima, in quanto esercitata sulla base di autorizzazione difforme da BAT Conclusions rilevanti ai fini di tale attività o in violazione di queste ultime»).

A fronte di ormai isolate pronunce che rimandano a risalenti arresti, che richiedono una "gestione totalmente difforme dall'attività autorizzata"[22] (probabilmente influenzate dalla contigua materia urbanistica, dove la totale difformità è espressamente equiparata alla mancanza di autorizzazione).

Questo è l'aspetto più complesso, che ha creato maggiori contrasti in dottrina e giurisprudenza.

Sotto il profilo "quantitativo", l'attività illecita non deve necessariamente essere "esclusiva", ben potendosi accompagnare ad attività lecita ed autorizzata[23].

Sotto il profilo "temporale", «il carattere "abusivo" di una attività organizzata di gestione dei rifiuti, tale da integrare il delitto, è configurabile quando si svolga continuativamente nell'inosservanza delle prescrizioni delle autorizzazioni»[24].

Sotto il profilo "qualitativo" occorrerà poi verificare che le violazioni non siano meramente "formali", ma integrino sostanziali violazioni dell'autorizzazione[25].

Ai fini della valutazione dell'abusività della condotta per violazione delle prescrizioni imposte nel titolo autorizzativo, occorrerà pertanto effettuare una valutazione unitaria che consideri l'aspetto temporale (continuatività dell'inosservanza), quantitativo (parte di attività svolta abusivamente rispetto a quella oggetto di autorizzazione) e qualitativo (natura formale o sostanziale delle violazioni riscontrate).

Il delitto è connotato dal c.d. "dolo specifico" del fine di conseguire un ingiusto profitto.

In proposito, è opportuno evidenziare come in una fattispecie di reato solo eventualmente plurisoggettiva (o a "concorso eventuale"), quale il delitto in parola, il concorrente nel reato risponderà non già direttamente per la violazione della norma incriminatrice, bensì per il combinato disposto della stessa con l'articolo 110 c.p.; in tal caso, il dolo del concorrente può essere generico e non specifico, e si concretizza nella semplice consapevolezza dell'illiceità della condotta altrui. Per la giurisprudenza è quindi sufficiente,

22) Cass. Pen., Sez. 3^, 18 maggio 2020, n. 15274.

23) Cass. Pen., Sez. 3^, 22 marzo 2011, n. 11488; Cass. Pen., Sez. 3^, 22 dicembre 2011, n. 47870 (in proc. Servizi Costieri s.r.l.) ha precisato che «la natura "abusiva" delle condotte non è esclusa dalla regolarità di una parte delle stesse allorché l'insieme delle condotte conduca ad un risultato di dissimulazione della realtà e comporti una destinazione dei rifiuti che non sarebbe stata consentita».

24) Cass. Pen., Sez. 3^, sentenza 24 febbraio 2017 n. 9133.

25) Cass. Pen., Sez. 3^, 8 gennaio 2008, n. 358, secondo cui «anche la difformità sostanziale della gestione dei rifiuti rispetto a quanto previsto dalle autorizzazioni concesse integra il requisito dell'abusività della condotta».

ai fini della configurabilità di un concorso punibile, che la particolare finalità presa in considerazione dalla legge penale sia perseguita almeno da uno dei soggetti che concorrono alla realizzazione del fatto. Si parla in tal caso di concorso "unilaterale"[26].

Quanto all'ingiusto profitto, occorre soffermarsi su due aspetti differenti: la "nozione di profitto" e quella di profitto "ingiusto".

Quanto al primo punto il profitto non deve necessariamente consistere in un ricavo patrimoniale, potendosi ritenere integrato anche dal mero risparmio di costi o dal perseguimento di vantaggi di altra natura senza che sia necessario, ai fini della configurazione del reato, l'effettivo conseguimento di tale vantaggio[27]. I vantaggi di altra natura possono consistere nel mantenimento o raggiungimento di una posizione apicale nell'ambito della struttura dirigenziale dell'azienda, ovvero in incentivi economici, con conseguente profitto personale e patrimoniale da parte degli interessati[28]. Sez. 3^, sentenza 2 marzo 2021 n. 8220 (in proc. Pistoia) ha infine precisato che il profitto «non deve assumere necessariamente carattere patrimoniale, potendo essere costituito anche da vantaggi di altra natura (cfr. Sez. 3, n. 53136 del 28/06/2017, Vacca, Rv. 272097-01, la quale ha ravvisato il vantaggio del trasporto illecito nello sgravio per le società appaltatrici degli oneri derivanti dalla regolarizzazione della movimentazione del materiale e nella maggiore celerità dei lavori di riqualificazione di un aeroporto internazionale, ma anche Sez. 4, n. 29627 del 21/04/2016, Silva, Rv. 267845-01)», e che «lo scopo di ottenere una commessa produttiva di significativi ricavi, concernente un'attività formalmente svolta in maniera lecita, perché supportata dalla titolarità delle necessarie autorizzazioni, ma nella consapevolezza della sua strumentalità allo smaltimento illecito di ingenti quantitativi di rifiuti, integri il fine di conseguire un ingiusto profitto richiesto dall'art. 260 d.lgs. n. 152 del 2006, e, attualmente, dall'art. 452-*quaterdecies* cod. pen.».

Il profitto è poi "ingiusto" qualora discenda da una condotta abusiva che, oltre ad essere "anticoncorrenziale", può anche essere produttiva di "conseguenze negative, in termini di pericolo o di danno, per la integrità dell'ambiente", impedendo il controllo da parte dei soggetti preposti sull'intera filiera dei rifiuti[29].

---

26) Cass. Pen., Sez. 6^, 20 gennaio 2004, n. 1271.
27) Cass. Pen., Sez. 3^, 10 novembre 2005, n. 40827.
28) Cass. Pen., Sez. 3^, 10 novembre 2005, n. 40828; recentemente, sez. 3^, 25 gennaio 2022, n. 2842.
29) Cass. Pen., Sez. 5^, 20 novembre 2019, n. 47076; Cass. Pen., Sez. 3^, 25 gennaio 2022, n. 2842, citata.

La contaminazione dei siti e gli illeciti in materia di discariche

di Rosalia Affinito*

1. I principi generali

Il diritto ambientale si contraddistingue per essere, ancora oggi, costituito da numerose norme di vario rango e provenienza tra loro non organicamente riunite, che si sono succedute nel corso degli anni ed "affastellate" senza una chiara visione di insieme, nate dalla necessità di dare attuazione a direttive comunitarie oppure dall'esigenza di dare una risposta efficace a fronte di condotte gravemente lesive dell'ambiente, in assenza di norme punitive connotate dalla necessaria tipicità e specialità.

L'unico testo organico è costituito dal decreto legislativo 152/2006 (TUA) che contiene unitariamente, ma in modo non completo, la disciplina in materia di rifiuti, acqua, suolo, aria; tuttavia, sono tuttora vigenti ulteriori discipline che regolamentano i suddetti settori specifici (ad esempio, continua ad essere in vigore in materia di discariche la legge 36/2003, novellata dal decreto legislativo 121/2020).

Una significativa novità normativa è costituita dalla legge costituzionale n. 1/22 che ha dato espresso rilievo costituzionale alla tutela dell'ambiente, della biodiversità e degli ecosistemi, anche nell'interesse delle future generazioni, interpolando gli articoli 9 e 41 della Costituzione. Nella loro attuale formulazione tali disposizioni pongono un limite alla iniziativa economico privata prevedendo che essa non possa svolgersi "*in modo da recare danno alla salute, all'ambiente, alla sicurezza, alla libertà, alla dignità umana*". L'articolo 41 prevede che la legge determini i programmi e i controlli opportuni perché l'attività economica pubblica e privata possa essere indirizzata e coordinata "*a fini sociali e ambientali*".

La materia ambientale, comunque, è in gran parte modellata dal formante comunitario, le direttive della Unione europea in uno con le sentenze della Corte di giustizia europea plasmano la materia; nel corso degli anni sono stati enucleati principi internazionalmente condivisi, recepiti nel diritto positivo dei diversi Paesi della Unione europea e sui quali si fonda la politica comunitaria. Si tratta dei seguenti principi:

a) "*Chi inquina paga – ma se ripara paga meno*", secondo il quale ogni

(*) Sostituto Procuratore della Procura della Repubblica presso il Tribunale di Roma.

fenomeno di inquinamento causato dall'uomo costituisce un deterioramento dell'ambiente che, non potendo essere economicamente valutabile in maniera corrispondente al reale danno, è stimato quanto meno pari alla spesa che occorre per il ripristino dello status quo ante o alla perdita di valore che il bene subisce. Ne sono espressione tutte quelle norme contenute nel testo unico ambiente in materia di tutela risarcitoria contenuta nella parte sesta a partire dagli articoli 299 e ss. del TUA e del codice penale, che impongono al responsabile della condotta illecita obblighi di bonifica e di ripristino ambientale (in particolare, vds. articolo 257 TUA, in materia di bonifica dei siti inquinati, e articolo 452-*duodecies* c.p.);

b) lo "sviluppo sostenibile" è principio a fondamento della politica ambientale, ad esso fanno riferimento gli articoli 9 e 41 della Costituzione e l'articolo 3-*quater* del Testo unico ambiente, secondo cui lo sviluppo che venga incontro a bisogni del presente non deve compromettere la capacità delle generazioni future di soddisfare i propri bisogni;

c) "il principio di prevenzione" che trova il suo riferimento normativo sempre nell'articolo 3-*ter* del TUA ed in diverse disposizioni in materia di bonifica. Esso deve essere osservato dagli enti pubblici preposte al rilascio della autorizzazione ed è finalizzato ad evitare i danni sin dall'origine, concretizzandosi in una previa valutazione dell'impatto sull'ambiente che potrebbero avere i progetti da autorizzare. È principio cui deve ispirarsi in particolar modo la pubblica amministrazione quando il rischio per l'ambiente sia scientificamente prevedibile e prevenibile con i mezzi della tecnologia, ed impone alle imprese di adottare tutte le precauzioni necessarie per impedire la concretizzazione di quel rischio secondo le BAT di settore (cioè le migliori tecniche disponibili a costi sostenibili - *best available techniques*);

d) "il principio di precauzione" opera ad un livello ancora più anticipato rispetto a quello di prevenzione, in quanto comporta l'adozione di misure cautelative per impedire o arginare il realizzarsi di danni ambientali che pur possibili non sono prevedibili: ad esso fa riferimento l'articolo 301 del TUA.

2. La disciplina in materia di contaminazione e di bonifica dei siti inquinati

La parte quarta del testo unico ambiente, segnatamente il titolo quinto, è dedicato alla disciplina degli interventi di ripristino ambientale dei siti contaminati e definisce le procedure, i criteri e le modalità per lo svolgimento delle operazioni necessarie per l'eliminazione e le riduzioni delle sorgenti di inquinamento, in conformità alla normativa europea e con particolare riferi-

mento al principio del "*chi inquina paga*". Gli eventi in grado di dare luogo alla contaminazione di suolo e acque, sia superficiali che sotterranee, possono essere i più svariati (dolosi o accidentali, puntuali o diffusi, istantanei o prolungati nel tempo, pregressi o tuttora attivi), così come diversi possono essere le sostanze contaminanti e l'estensione dell'area contaminata. In linea generale, comunque, i siti contaminati più complessi e problematici sono per lo più riconducibili ad eventi di contaminazione storica, ovvero risalenti ad alcuni decenni fa quando in Italia non era ancora stata emanata alcuna normativa a tutela dell'ambiente. Si tratta di vecchie aree industriali (sia dismesse che tuttora in attività) o discariche interrate incontrollate. L'esistenza dei siti contaminati non è sempre palese (sicuramente molti non sono noti): la contaminazione può essere scoperta accidentalmente – ad esempio a seguito di scavi edili o di lavori di manutenzione su impianti o serbatoi interrati – oppure essere rilevata sulla base di anomalie nelle concentrazioni delle acque sotterranee.

Ai sensi della vigente normativa viene definito "*sito potenzialmente contaminato*" un'area dove sono state riscontrate – in campioni di suolo superficiale, sottosuolo o di acqua sotterranea – concentrazioni di sostanze inquinanti, superiori a quelle massime previste dalla normativa; si tratta di siti in cui i valori delle sostanze inquinanti, indicati dalla Tab. I, All. 5, Titolo V, Parte IV del d.lgs. 152/06, sono superiori alle cosiddette CSC (acronimo di concentrazione soglie di contaminazione), anche per un solo parametro.

Quando a seguito di specifici approfondimenti si accerta la presenza di rischio per la salute umana derivante dall'inquinamento l'area in esame viene definita "sito contaminato".

Dal dato normativo emerge con chiarezza la distinzione tra la nozione di concentrazione soglie di contaminazione (CSC) e quella di concentrazione soglie rischio (CSR); le prime sono strumentali a riconoscere nell'area sottoposta a verifica l'esistenza di sostanze inquinanti in una soglia tale da giustificare la predisposizione di un piano di caratterizzazione; le seconde sono preordinate alla verifica della sussistenza di un livello di rischio tale da giustificare l'attuazione di interventi di bonifica e di messa in sicurezza.

La fissazione dei valori di CSC non ha per scopo la tutela della salute, ma solo la rintracciabilità nell'ambiente delle sostanze potenzialemnte inquinanti: per contro, la soglia "di intervento" (questa, beninteso, potenzialmente onerosa per il responsabile dell'inquinamento che vi fosse onerato) è fissata in un secondo momento, avuto riguardo ai limiti fissati per la tutela della salute dall'Organizzazione Mondiale della Sanità

Sul piano della rilevanza penale di questi fatti, costituisce un punto fer-

mo in giurisprudenza l'affermazione secondo cui il superamento delle CSC non è sufficiente per integrare il reato di inquinamento ambientale punito dall'art. 452-*bis* c.p. Nella decisione n. 50018/18 la Cassazione sviluppa considerazioni di estremo interesse sulla complicata questione del rapporto tra accertamento dell'evento inquinante e superamento dei limiti soglia previsti dal codice dell'ambiente. Il caso concreto riguardava l'abusivo sversamento in una cava dismessa di centinaia di migliaia di metri cubi di rifiuti speciali di svariata natura e, nel corso delle indagini, il pubblico ministero aveva affidato ad un consulente tecnico l'incarico di verificare la qualità del suolo interessato dall'interramento di rifiuti. Tale verifica aveva evidenziato il superamento delle concentrazioni soglia di contaminazione (CSC) per siti ad uso verde pubblico, privato e residenziale in relazione a numerose sostanze inquinanti ricomprese nell'elenco di cui alla Tab. I, All. 5, Titolo V, Parte IV del d.lgs. 152/06, la maggior parte delle quali compatibili con la composizione dei rifiuti interrati. Sulla scorta di tali risultati, il consulente del pubblico ministero aveva quindi concluso che il sito doveva considerarsi come "potenzialmente contaminato", espressione che, nel lessico del codice dell'ambiente, identifica un sito nelle cui matrici ambientali sono state rinvenute sostanze inquinanti in concentrazioni superiori alle CSC, cioè ai valori di "concentrazione delle soglie di contaminazione", ma sul quale non sono ancora state espletate le operazioni di caratterizzazione e di "analisi di rischio sanitario e ambientale sito specifiche", necessarie per calcolare le concentrazioni soglia di rischio (CSR), dal cui eventuale superamento dipende la qualificazione del sito come "contaminato".

In sede di ricorso l'indagato aveva sostenuto che una contaminazione meramente "potenziale", come quella accertata dal consulente del p.m., non sarebbe sufficiente né idonea ad integrare gli estremi del delitto di inquinamento ambientale. La Cassazione nella decisione richiamata ha ritenuto, invece, che le definizioni contenute all'art. 240 TUA – tra cui quelle di "sito potenzialmente contaminato" e di "sito contaminato" – essendo finalizzate a disciplinare un'attività, la bonifica di siti contaminati, che per espressa volontà del legislatore deve essere condotta tenendo conto dei profili di rischio per la salute umana derivanti dall'esposizione prolungata all'azione delle sostanze presenti nelle matrici ambientali contaminate, non possono essere richiamati per definire gli elementi costitutivi del delitto di inquinamento ambientale (introdotto dalla successiva l. 68/15) che ha come oggetto di tutela penale "l'Ambiente" in quanto tale ed al quale è tendenzialmente estranea la protezione della salute pubblica. Secondo i giudici di legittimità, dunque, il dato del superamento delle CSR, imprescindibile per poter considerare un

sito contaminato secondo le disposizioni in materia di bonifica previste dal TUA, non è necessario per affermare la sussistenza dell'evento inquinante previsto dall'art. 452 cod. pen.

3. Le procedure per l'accertamento del superamento delle soglie di contaminazione

Al verificarsi di un evento potenzialmente contaminante (es. sversamento accidentale, rottura di una cisterna) o al rinvenimento di contaminazione storiche, il soggetto responsabile (nel caso di evento accidentale) o il proprietario del sito (nel caso di contaminazione storica), devono, alternativamente, provvedere a dare comunicazione della potenziale contaminazione all'autorità amministrativa (regione, provincia e comune) e se si tratta del responsabile dell'inquinamento deve procedere anche alla contestuale messa in opera delle necessarie misure di prevenzione. Nel caso in cui non lo faccia commette il reato previsto punito dall'articolo 257 TUA. Alla preliminare attività di messa in sicurezza deve seguire un'indagine sul superamento delle concentrazioni soglia di contaminazione (CSC), previste dall'allegato 5 della Parte IV del TUA, avviate dal responsabile dell'inquinamento e non soggette ad approvazioni dell'autorità amministrativa. All'esito delle indagini, se le concentrazioni risultano nei limiti ci si limita al ripristino del sito; invece, se risultano superate il procedimento prosegue ed il responsabile dell'inquinamento è obbligato a mettere in sicurezza la zona e deve effettuare le dovute comunicazioni al comune ed alle province competenti per territorio, e per i siti di interesse nazionale (SIN) anche al Ministero dell'Ambiente. Il solo responsabile dell'evento inquinante, nella seconda fase, entro trenta giorni, deve predisporre un "piano di caratterizzazione" che necessita dell'approvazione della regione, in attuazione del quale bisogna applicare al sito una procedura di "analisi del rischio per la determinazione delle concentrazioni soglia rischio (CSR)", le cui risultanze devono essere presentate alla regione nei successivi sessanta giorni.

Il piano della caratterizzazione (descritto e disciplinato dall'allegato 2 alla parte IV del citato decreto legislativo) è, dunque, un documento progettuale riportante un elenco di attività di indagine ed i tempi necessari per effettuarle, compiute le quali si potrà conoscere l'impatto sulle matrici ambientali (suolo, sottosuolo, acque sotterranee e superficiali). Solo con i risultati del piano di caratterizzazione del sito è possibile prevedere la necessità o meno della predisposizione del progetto operativo di bonifica, anche in base all'analisi di rischio sito-specifica per la definizione delle concentrazioni di rischio.

In sostanza, con le risultanze del piano della caratterizzazione si può progettare la bonifica, ma a tal fine è necessario preventivamente verificare la distribuzione delle concentrazioni di sostanze inquinanti al di sopra dei valori di Concentrazione delle Soglie di Contaminazione.

In sede di approvazione del piano di caratterizzazione si devono indicare i valori delle soglie di contaminazione (CSC) cioè i valori minimi che servono a riconoscere l'esistenza delle sostanze, ossia a "vederle"; dopo di che, in fase di progettazione della bonifica, si determineranno i valori delle soglie di rischio (CSR), cioè le concentrazioni degli inquinanti che non causano rischio per l'uomo e l'ambiente e che per questo sono accettabili. Per contro, la soglia "di intervento" (questa, beninteso, potenzialmente onerosa per il responsabile dell'inquinamento che vi fosse onerato) è fissata in un secondo momento, avuto riguardo ai limiti individuati per la tutela della salute dall'Organizzazione Mondiale della Sanità.

Per le sostanze potenzialmente inquinanti ma non tabellate, il Consiglio di Stato ha ritenuto che "*per la determinazione della soglia di concentrazione rilevante per le sostanze inquinanti non tabellate non appare arbitraria, per un verso, l'utilizzazione di parametri fissati per sostanze con analoghe caratteristiche e, per altro verso, la valorizzazione del parere reso dall'Istituto di superiore di sanità, al quale la Regione (e l'ARPA) hanno inteso correttamente adeguarsi, senza che all'uopo fosse necessaria (non trattandosi di prefigurare le condizioni per la programmazione di un intervento) una apposita motivazione*" (CDS 2019/236).

Nel caso in cui l'analisi del rischio dimostri che le concentrazioni dei contaminanti presenti sono superiori ai valori soglia-rischio, il responsabile deve formulare un progetto di bonifica da sottoporre entro sessanta giorni alla regione per l'approvazione. E la mancata esecuzione di questo specifico progetto la sola circostanza che costituisce omessa bonifica ai fini del perfezionamento della fattispecie criminosa di cui all'art. 257 TUA.

4. Cenni sui reati di "omessa bonifica"

Nell'ambito del diritto penale ambientale il tema delle bonifiche è considerato trasversale in quanto riferita a tutti e tre i settori – acqua, arie, rifiuti – sulla cui tutela è basata la normativa del testo unico.

L'art. 240, 1 comma, lett. p) TUA definisce la bonifica come "*l'insieme degli interventi atti a eliminare le fonti di inquinamento e le sostanze inquinanti o a ridurre le concentrazioni delle stesse presenti nel suolo, nel sottosuolo e nelle acque sotterranee ad un livello uguale o inferiori ai valori delle*

contaminazioni soglie di rischio".

L'omissione dell'obbligo di bonificare costituisce il presupposto di fatto per l'integrazione di due fattispecie incriminatrici: una di tipo contravvenzionale prevista dall'art. 257 TUA, e l'omonimo delitto di "Omessa bonifica" di cui all'art. 452-*terdecies* c.p., introdotta con legge 68/2015.

La fattispecie contravvenzionale della omessa bonifica si configura solo quando il soggetto che abbia cagionato un inquinamento, qualificato dal superamento della concentrazione di una soglia di rischio, ometta di dare esecuzione al provvedimento di bonifica approvato dall'autorità amministrativa all'esito del procedimento descritto dagli artt. 242 e ss. TUA. Il secondo comma prevede una circostanza aggravante laddove la contaminazione sia stata provocata da sostanze pericolose[1].

L'omessa bonifica che perfeziona il reato in esame non è, dunque, da intendere come una qualsiasi bonifica del sito contaminato, ma bensì come l'astensione dall'obbligo di esecuzione di uno specifico progetto di bonifica approvato all'esito del procedimento di cui all'art. 242 TUA.

Con sentenza del 2018/17813 la Cassazione ha stabilito che il reato di omessa bonifica dei siti inquinati è configurabile non solo nel caso in cui il soggetto obbligato non vi provveda in conformità al progetto approvato dall'autorità competente, nell'ambito del procedimento di cui all'art. 242 e ss. del d.lgs. 3 aprile 2006, n. 152, ma anche in quello in cui impedisca la stessa formazione del progetto di bonifica e, quindi, la sua realizzazione, non attuando il piano di caratterizzazione necessario per la predisposizione del piano di bonifica.

Alla luce della normativa sopradescritta[2], viene immediatamente in evidenza la difficoltà di applicazione pratica di questa disciplina dal momento che il reato sembra non si perfezioni se non nel caso di mancata esecuzione del progetto di bonifica; progetto che, a ben vedere, deve essere formulato dallo stesso responsabile dell'inquinamento all'esito di tutta la procedura di cui all'art. 242 che ha inizio proprio con la comunicazione della potenziale contaminazione cui è obbligato lo stesso responsabile dell'inquinamento. Se da un lato, dunque, ci si chiede retoricamente quale probabilità vi sia che il responsabile della contaminazione del sito dia avvio ad un procedimento che comporta per lui una serie di oneri e una responsabilità penale nel caso

1) La formula sostanze pericolose va riferita: per i rifiuti, a quelli indicati come tali tramite asterico nell'allegato D della parte V del TUA; per le sostanze contenute negli scarichi idrici, a quelle indicate nelle tabelle 5 e 3/A dell'allegato 5 della parte III del TUA, cui rinvia l'art. 137 TUA.

2) Per una migliore comprensione, vedi schema in A. Di Landro, *Bonifiche: Il labirinto della legislazione ambientale: dove le responsabilità penali si perdono*, in *penalecontemporaneo.it*, 28 febbraio 2014, p. 17.

in cui non si attenga al progetto di bonifica finale; dall'altro, ci si interroga sulla configurabilità o meno del reato in esame nel caso in cui il responsabile dell'inquinamento avvii la procedura di cui all'art. 242 TUA ma non porti a termine tutte le tappe procedimentali e, dunque, non giunga a sottoporre all'autorità amministrativa il progetto di bonifica. Su quest'ultimo punto la giurisprudenza ha registrato un contrasto, ma nella maggior parte dei casi esaminati il giudice di legittimità ha ritenuto che in assenza del progetto di bonifica di cui all'art. 242 TUA non possa configurarsi il reato in esame; altrimenti vi sarebbe una lesione del principio di legalità nella sua declinazione di divieto di analogia in materia penale[3].

Nonostante la formulazione dell'art. 257 TUA appaia apparentemente aperta alla punibilità di qualsiasi soggetto che cagioni la contaminazione di un sito, la giurisprudenza dominante ricostruisce la contravvenzione di omessa bonifica come reato proprio che può essere compiuto solo dal responsabile dell'inquinamento[4]. Alla stessa conclusione arriva la dottrina maggioritaria sia che parta dalla qualificazione della fattispecie come omissiva propria, sia che la consideri un reato commissivo di evento. Infatti, anche in tale ultima ipotesi, viene negato che il reato possa essere compiuto per omissione ex art. 41 comma 2 c.p. da un soggetto diverso dal responsabile dell'inquinamento, non rinvenendosi nell'alveo della normativa attuale alcuna posizione di garanzia gravante su un soggetto diverso.

La normativa del T.U.A., infatti, descrive il responsabile dell'inquinamento come l'unico soggetto su cui possa gravare l'obbligo a bonificare imposto dall'autorità amministrativa. Persino l'intervento del proprietario o gestore del fondo è ricostruito dall'art. 245 TUA in termini di mera facoltatività; la disposizione di cui all'art. 242, comma 1, TUA[5] – che estende l'applicazione della procedura di bonifica prevista per il responsabile dell'inquinamento al caso di contaminazioni storiche che possano comportare rischi di aggravamento – non può essere intesa come norma che implicitamente stabilisca un obbligo di bonifica in capo al proprietario del fondo, pena la lesione del divieto vigente in materia penale di analogia *in malam partem*. L'articolo in questione deve essere interpretato semplicemente come norma che equipara la posizione del responsabile dell'inquinamento a quella del proprietario

3) Cass. Pen., Sez. III, n. 22006 del 13.4.2010.
4) V. Cass. pen., Sez. III, 11/5/2011 n. 18503, Burani.
5) Art. 242, 1 comma TUA: «Al verificarsi di un evento che sia potenzialmente in grado di contaminare il sito, il responsabile dell'inquinamento mette in opera entro ventiquattro ore le misure necessarie di prevenzione e ne dà immediata comunicazione ai sensi e con le modalità di cui all'articolo 304, comma 2. *La medesima procedura si applica all'atto di individuazione di contaminazioni storiche che possano ancora comportare rischi di aggravamento della situazione di contaminazione*».

dell'area ai soli fini dell'obbligo di comunicazione all'autorità; obbligo peraltro sanzionato – secondo la dottrina maggioritaria – soltanto amministrativamente ai sensi dell'art. 304, comma 2 TUA[6].

5. Il reato di omessa bonifica di cui all'art. 452-*terdecies* c.p.

Questa fattispecie di reato è stata introdotta all'interno del codice penale dalla legge 68/2015 e si aggiunge alla fattispecie contravvenzionale prevista dal TUA ed agli altri reati ambientali già disciplinati in altre sedi. La clausola di salvezza presente in apertura della nuova disposizione attribuisce alla nuova fattispecie un ruolo di chiusura del sistema di tutela penale dell'ambiente.

Ciò nonostante, la nuova fattispecie delittuosa codicistica trova un campo di applicazione particolarmente ampio visto che l'obbligo di bonifica ivi richiamato può avere fonte non solo in un provvedimento dell'autorità amministrativa, ma anche in una legge o in un ordine del giudice. A ciò si deve aggiungere che, anche con riguardo agli ordini delle autorità amministrative, trova più spesso applicazione la nuova fattispecie codicistica che le fattispecie precedenti apparentemente concorrenti, posto che la clausola di apertura dell'art. 452-*terdecies* c.p. fa salva l'applicazione delle sole norme incriminatrici che prevedono un reato più grave ed i reati previsti dal TUA hanno più spesso natura contravvenzionale (art. 257, contravvenzione di omessa bonifica; art. 255, comma 3, TUA, contravvenzione che punisce la violazione dell'ordinanza di bonifica adottata dal sindaco di cui all'art. 192, comma 3, TUA).

Problemi di interferenza tra le due fattispecie di omessa bonifica si pongono solamente rispetto all'ipotesi in cui la bonifica sia disposta per ordine dell'autorità amministrativa tramite l'approvazione in conferenza di servizi del progetto di bonifica formulato dal responsabile dell'inquinamento all'esito del procedimento di cui all'art. 242 TUA.

In relazione a tale caso, si sono sviluppate in dottrina diverse teorie, ovvero secondo:

a) una prima interpretazione, come anticipato, le due norme incriminatrici sono in un rapporto di concorso apparente tra loro che trova risoluzione nella clausola di salvezza di cui all'art. 452-*terdecies* c.p., la quale fa salvi solo i reati più gravi. Dunque, prevale la fattispecie codicistica su quella contravvenzionale di cui all'art. 257 TUA spazi di operatività per quest'ultima

6) Secondo una dottrina minoritaria invece anche il proprietario del fondo che non abbia cagionato l'inquinamento potrà rispondere della contravvenzione di omessa comunicazione della potenziale contaminazione all'autorità ai sensi dell'art. 257, 1 comma, ultimo periodo T.U.A. Per argomentazioni V. A. Di Landro, *Bonifiche: Il labirinto*..., cit., p. 11.

sarebbero ravvisabili, dunque, soltanto nelle ipotesi di omessa bonifica colposa, ossia non eseguite correttamente per negligenza o imperizia, ma non in maniera volontaria;

b) un'altra parte della dottrina, invece, opera il principio di specialità di cui all'art. 15 c.p. nella risoluzione del conflitto apparente di norme e, dunque, prevale la fattispecie di cui all'art. 257 TUA in tutti i casi in cui l'omessa bonifica sia esattamente il risultato della mancata esecuzione del progetto di bonifica approvato dalla pubblica amministrazione all'esito della procedura di cui all'art. 242 TUA o dell'esecuzione della bonifica in maniera difforme rispetto a questo progetto. Troverebbe, al contrario, applicazione la nuova fattispecie codicistica nei casi in cui l'omessa bonifica sia piuttosto sia conseguenza dell'omissione di una o di tutte le fasi procedimentali di cui all'art. 242 TUA precedenti alla redazione del progetto.

Si tratta di un reato proprio, che può essere commesso dal responsabile dell'inquinamento.

Controversa risulta, invece, l'applicabilità della fattispecie al proprietario dell'area inquinata. Dal dettato normativo sembrerebbe, infatti, astrattamente configurabile il reato in capo a chiunque sia soggetto dell'obbligo di bonifica previsto dalla legge, dal giudice o dalla pubblica autorità. Tuttavia, a ben vedere, nel caso in cui l'obbligo nei confronti del proprietario dell'area sorga per effetto di un provvedimento dell'autorità amministrativa ai sensi dell'art. 244 TUA, la responsabilità penale in capo a questi andrebbe esclusa per illegittimità del provvedimento. Infatti, il Codice dell'ambiente (articolo 240) è chiaro nel prevedere che tale provvedimento può essere emesso solo nei confronti del responsabile dell'inquinamento, che le autorità amministrative hanno il compito di ricercare ed individuare; dovendo queste altri enti effettuare direttamente la bonifica.

Del pari, la giurisprudenza amministrativa ha in modo constante escluso che sussista l'obbligo di effettuare la bonifica in capo al proprietario dell'area; di recente il Consiglio di Stato (sez. II, 1 settembre 2020, n. 5340)[7] ha ribadito che non può imporre al proprietario di un'area inquinata, che non sia anche l'autore dell'inquinamento, l'obbligo di porre in essere le misure di messa in sicurezza di emergenza e bonifica, ha chiarito che il Codice dell'ambiente (articolo 253) prevede una responsabilità solo patrimoniale del proprietario incolpevole del suolo su cui insistono rifiuti pericolosi, salvi gli oneri relativi agli interventi di urgenza e la facoltà di eseguire spontaneamente gli interventi di bonifica ambientale. Non è cioè configurabile in via auto-

7) A. Zuco, *Imposizione degli obblighi di bonifica al responsabile dell'inquinamento e facoltà in capo al proprietario e/o gestore dell'area*, in *studiolegalezuco.it*.

matica, in maniera oggettiva, per posizione o per fatto altrui, una responsabilità in capo al proprietario dell'area inquinata e da bonificare per il solo fatto di rivestire tale qualità, ove non si dimostri il suo apporto causale colpevole al danno ambientale riscontrato (cfr. *ex multis* Cons. Stato, sez. VI, 21 marzo 2017, n. 1260).

La stessa regola non vale tuttavia avuto riguardo alle conseguenze patrimoniali dell'intervento surrogatorio cui l'Ente proprietario sia comunque costretto dall'esigenza di preservare l'ambiente, e con esso la salute pubblica, dai pericoli rivenienti da una riscontrata contaminazione.

Dalle disposizioni contenute nel d.lgs. n. 152/2006, possono dunque ricavarsi le seguenti regole:

– gli interventi di riparazione, messa in sicurezza, bonifica e ripristino gravano esclusivamente sul responsabile della contaminazione, cioè sul soggetto al quale sia imputabile, almeno sotto il profilo oggettivo, l'inquinamento;

– ove il responsabile non sia individuabile o non provveda (e non provveda spontaneamente il proprietario del sito o altro soggetto interessato), gli interventi che risultino necessari sono adottati dalla P.A. competente;

– le spese sostenute per effettuare tali interventi potranno essere recuperate, sulla base di un motivato provvedimento (che giustifichi, tra l'altro, l'impossibilità di accertare l'identità del soggetto responsabile ovvero quella di esercitare azioni di rivalsa nei confronti del medesimo soggetto ovvero la loro infruttuosità), a mezzo di azione in rivalsa verso il proprietario, che risponderà nei limiti del valore di mercato del sito;

– a garanzia di tale diritto di rivalsa, il sito è gravato di un onere reale e di un privilegio speciale immobiliare.

Bibliografia essenziale

Amendola, *Il nuovo delitto di "omessa bonifica": primi appunti*, in *lexambiente.it*, 30 ottobre 2015

Di Landro, *Bonifiche: Il labirinto della legislazione ambientale: dove le responsabilità penali si perdono*, in *penalecontemporaneo.it*, 28 febbraio 2014, p. 17

Ficco (a cura di), *Gestire i rifiuti tra legge e tecnica*, Ed. IX, Milano, 2022

Fimiani, *La tutela penale dell'ambiente*, Ed. IV, Milano, 2022

Galanti, *I delitti contro l'ambiente - Analisi normativa e prassi giurisprudenziali*, Pacini Giuridica, 2021

Id., *Obblighi di ripristino/bonifica e successione tra amministratori dell'ente: la questione della responsabilità penale del soggetto subentrante*, in *tuttoambiente.it*, 18 maggio 2020

Id., *Reato di omessa bonifica e D.lgs. n. 231/2001: la bonifica giova (anche) all'ente?* in *lexambiente.it*, 11 giugno 2012

Onofrj, *Proposta per una direttiva del Parlamento europeo e del Consiglio sulla protezione dell'ambiente attraverso il diritto penale: nuove frontiere nella lotta ai crimini ambientali in Europa*, in *sistemapenale.it*, 5 luglio 2022

Ramacci, *Diritto penale dell'ambiente*, Piacenza, 2021

Ruga Riva, *Diritto penale dell'ambiente*, ed. IV, Torino, 2021

La tutela amministrativa per la protezione ambientale e l'uso dell'intelligenza artificiale

di Giuseppe Sgorbati*

1. Introduzione: la struttura territoriale italiana per la protezione dell'ambiente – Il contesto amministrativo, le attività tecniche

Al fine di descrivere l'uso di tecnologie innovative per la protezione dell'ambiente nel settore pubblico, e per proiettarne nel tempo i possibili sviluppi, è opportuno richiamare brevemente il contesto istituzionale che ha visto il loro sviluppo: il Sistema Nazionale per la Protezione dell'Ambiente (SNPA).

Le competenze pubbliche di protezione dell'ambiente in Italia sono gestite, in via ordinaria, dalle componenti del SNPA, istituto con la legge 28 giugno 2016, n. 132, che la struttura di rete che unisce le Agenzie per la protezione dell'ambiente regionali e delle provincie autonome (ARPA - APPA) e l'Istituto superiore per la protezione e la ricerca ambientale.

La norma sistematizza le funzioni attribuite al SNPA, tra le quali, principalmente, si collocano:

- la determinazione degli standard di qualità ambientale;
- la regolazione delle imprese;
- la persecuzione dei crimini ambientali.

Ognuna di queste attività è svolta nel quadro di provvedimenti che recepiscono il complesso delle direttive dell'Unione europea[1], che ritiene che l'uniforme livello di protezione ambientale in Europa costituisca un diritto fondamentale dei propri cittadini ma anche un importante elemento di tutela della concorrenza tra le imprese nei diversi Paesi dell'Unione, dati i costi aggiuntivi introdotti nei cicli produttivi dal contenimento delle emissioni.

La regolazione delle imprese è attuata dalle autorità quali i Comuni, le Aree Metropolitane, lo Stato, a cui sono attribuiti poteri di carattere amministrativo. Le attività tecniche correlate, sia al fine del rilascio delle autorizzazioni, sia per la verifica del loro rispetto, sono poste principalmente in capo alle varie componenti del SNPA.

Lo svolgimento delle attività per la verifica del rispetto del contenuto

(*) Già direttore di ARPA Lombardia, Prof. Bicocca, Milano.

1) Le direttive dell'Unione europea sono recepite, in Italia, attraverso il "Testo Unico sull'Ambiente": il decreto legislativo 3 aprile 2006, n. 152 "Norme in materia ambientale" e s.m.i.

degli atti autorizzativi e, in generale, del rispetto della legislazione ambientale applicabile, viene svolta dalle Agenzie Ambientali e dall'ISPRA nel loro ruolo di polizia amministrativa.

In caso della individuazione della potenziale presenza di reati ambientali di rilievo penale, la situazione viene segnalata all'Autorità giudiziaria, che prosegue le indagini avvalendosi di Agenti di polizia giudiziaria, che possono anche essere presenti tra il personale ispettivo del SNPA.

Ciò crea un primo punto di contatto tra la giurisdizione penale ambientale e le componenti del SNPA, che ne proietta le attività oltre le funzioni di polizia amministrativa.

Un ulteriore punto di contatto è rappresentato dalla collaborazione tecnica offerta dalle componenti del SNPA nei confronti dei vari poteri e forze dello stato nel contrasto ai crimini ambientali.

Il ruolo del SNPA è, anche nel caso di crimini ambientali in atto, di supporto tecnico alla giurisdizione, specie lo studio delle conseguenze sull'ambiente dell'attività illegale, per il contenimento dei suoi effetti e ai fini della quantificazione del danno ambientale nei procedimenti e nei giudizi civili, penali e amministrativi. Non è escluso un importante contributo per l'accertamento delle responsabilità, anche attraverso lo svolgimento di accertamenti tecnici.

Il SNPA, di fronte a ripetute e gravi situazioni ambientali generate da azioni criminali, ha comunque deciso di sperimentare attività di carattere preventivo, utilizzando le competenze tecnologiche sviluppate nel settore del monitoraggio ambientale, per l'implementazione di tecniche di sorveglianza del territorio a presidio contro i crimini ambientali.

2. La sorveglianza del territorio attraverso l'osservazione terrestre: le origini e gli sviluppi

Il caso che ha attivato, in tempi recenti, lo studio e la ricerca applicata sull'uso dell'Osservazione Terrestre e dell'Intelligenza Artificiale è il fenomeno degli incendi di impianti per la gestione dei rifiuti o altri accumuli illegali in Lombardia, avvenuto negli scorsi anni.

Sebbene il fenomeno degli incendi in depositi di rifiuti, legali o meno, sia da considerare storico, attorno al 2017 esso ha avuto, in tutta Italia, una particolare intensificazione.

Tra le varie cause della situazione si ritrova la saturazione del mercato dei materiali da raccolta differenziata destinati al riciclaggio, ulteriormente aggravata dal divieto elevato dalla Cina all'importazione delle "plastiche da

riciclo", deciso da Pechino nel 2017; la Cina, a quella data, assorbiva oltre il 72% della produzione a livello globale di questo tipo di materiale.

Ciò ha aperto spazi e profitti enormi per lo smaltimento illegale di questo tipo di rifiuti, ovviamente senza alcuna cura per l'ambiente.

Dopo alcuni importanti incendi in Lombardia, l'ARPA della regione ha deciso di effettuare uno studio di fattibilità per determinare l'utilità dell'uso dell'osservazione terrestre quale strumento di prevenzione del fenomeno degli incendi e di altre forme di criticità ambientali.

Infatti, alcune analisi retrospettive di immagini terrestri[2], acquisite da satellite e da sorvoli aerei in siti che avevano subito incendi, hanno dimostrato che, frequentemente, sarebbe stato possibile individuare situazioni critiche prodromiche agli incendi, quali palesi irregolarità gestionali ed eccesso di accumulo di materiali; è stata inoltre verificato come l'analisi di immagini satellitari permettesse di identificare la presenza di rifiuti in aree aperte ed in siti abbandonati.

Sulla base di tale evidenza, è stato sviluppato il progetto *Sorveglianza Avanzata Gestione Rifiuti* (SAVAGER)[3].

Il Progetto è stato applicato sperimentalmente nel 2019 alla provincia di Pavia[4] per la ricerca di depositi illegali di rifiuti attraverso l'analisi da parte di operatori specializzati di immagini terrestri. I risultati della sperimentazione sono risultati estremamente significativi, ma contemporaneamente hanno aperto una serie di quesiti sull'organizzazione per la gestione delle informazioni acquisite, anche in rapporto alla giurisdizione.

L'analisi del territorio della provincia di Pavia ha dimostrato una notevole prolificità della tecnica (580 siti critici individuati nella prima sessione della sperimentazione) e ha sollevato il quesito di come gestire una simile massa di potenziali notizie di reato. A questo fine è stato sviluppato un apposito protocollo di intesa tra la Procura della Repubblica presso il Tribunale di Pavia ed ARPA Lombardia per la definizione di una modalità condivisa di gestione degli esiti dell'analisi territoriale, con l'integrazione di risorse dei due Soggetti sottoscrittori.

L'accordo ha previsto uno studio e selezione comune dei siti sospetti su

2) Nella fase preliminare del progetto sono state impiegate immagini terrestri acquisite attraverso piattaforme *open source*, es.: Google Earth Pro; è stato studiato l'uso delle immagini acquisite nell'ambito del programma dell'Unione europea Copernicus, sia nel visibile che in altre bande spettrali ed acquisite con tecnica Synthetic Aperture Radar (SAR), anch'esse di libero accesso.

3) Il progetto SAVAGER (Sorveglianza Avanzata Gestione Rifiuti) è stato approvato e finanziato dalla Direzione Generale Ambiente e Clima di Regione Lombardia con decreto n. 4129 del 27/03/2019.

4) La provincia di Pavia è caratterizzata dalla presenza 63 Comuni distribuiti su una superficie di 1.347 km^2.

cui effettuare ispezioni con il coinvolgimento delle strutture più tradizionali.

L'estensione della sperimentazione ad altri territori della Lombardia e l'implementazione di analoghe modalità di gestione dell'informazione grezza derivante dal primo screening hanno portato, al 2021, al quadro operativo complessivo di seguito riassunto:

Fase	Risultato	
Sorveglianza	Percentuale del territorio regionale potenzialmente critico analizzato:	50%
	Siti potenzialmente critici rilevati	n. 3.789
Selezione	Siti critici con alta priorità di indagine	n. 402
Controllo (*in progress*)	Siti critici selezionati per il controllo diretto	n. 80
	Siti controllati	n. 57
	Percentuale dei siti controllati costituiti da impianti autorizzati	28%
	Percentuale dei siti controllati costituiti da situazioni non autorizzate	72%
Esiti del controllo	Nessuna criticità	14%
	Non conformità senza necessità di sequestro dell'area	44%
	Non conformità con sequestro dell'area	42%

È da sottolineare l'elevata efficienza del sistema, rappresentata dall'alto numero di siti sospetti individuati, contemperata da elevata efficacia, dopo selezione, nel contrasto all'illegalità: l'86% dei siti selezionati controllati si sono rivelati non conformi; il risultato, in termini di ottimizzazione nell'impiego delle risorse ispettive, è estremamente significativo, specie nella situazione di perdurante criticità di disponibilità di risorse, sia nella giurisdizione sia, in generale, nelle attività di protezione ambientale.

Il progetto SAVAGER è stato confermato ed è recentemente passato alla fase di impiego ordinario[5]. In seguito alla identificazione di siti poten-

5) È prevista la possibilità di accedere ad immagini satellitari commerciali ad alta risoluzione *on demand*, con tempi di latenza dell'ordine generalmente inferiori alla settimana, a titolo oneroso.

zialmente critici può essere pianificato un sorvolo, in accordo con la Polizia Giudiziaria, con droni o altri mezzi aerei, per acquisire informazioni di maggiore dettaglio, anche in modo riservato. Il supporto di droni è poi utile in fase ispettiva per interventi mirati e per l'acquisizione di immagini che permettono la ricostruzione digitale 3D dei siti e la stima di volumi di accumuli o cavità con precisione migliore dell'1% e con tempi di rilievo e di elaborazione dell'ordine di poche ore.

Il controllo dello stato dei luoghi prima di ispezioni programmate è inoltre di supporto per la pianificazione degli interventi di controllo ordinari.

3. L'impiego di tecniche di Intelligenza Artificiale nelle indagini ambientali: l'osservazione terrestre

Lo sviluppo logico dell'attività di indagine ambientale attraverso analisi di immagini terrestri è consistito nell'applicazione di sistemi di analisi automatica delle immagini, basati su tecniche di Intelligenza Artificiale, per l'individuazione di situazioni di illegalità, in sostituzione dell'intervento umano.

Ciò comporta un netto risparmio di risorse umane qualificate ed ha aperto la possibilità di un regolare screening periodico del territorio, ai fini di individuazione, ma anche di prevenzione e deterrenza, dei crimini ambientali.

Nel caso del progetto SAVAGER, ARPA Lombardia è stata affiancata dal Politecnico di Milano per l'implementazione di un sistema per il rilevamento di siti di discarica nelle immagini aeree attraverso analisi e categorizzazione delle immagini basato su modelli di classificazione delle scene con l'uso di una rete neurale convoluzionale (CNN), un campo ancora poco esplorato.

L'attività ha richiesto un "addestramento" dell'algoritmo di Intelligenza Artificiale per l'identificazione automatica di possibili situazioni illegali.

A questo scopo, è stato creato un set di dati specifico: 3.000 immagini di cui il 33% erano relative a siti con presenza accertata di situazioni illecite, quali campioni positivi.

Tali siti positivi erano stati individuati in precedenza da esperti che hanno esaminato direttamente le ortofoto delle zone di interesse acquisite nel corso del 2018[6].

Il sistema ha dimostrato un'elevata affidabilità, sia in termini di basso rateo sia di falsi negativi che di falsi positivi.

---

6) Cfr. Torres - Fraternali, *Learning to Identify Illegal Landfills through Scene Classification in Aerial Images*, in *Remote Sens*., 2021, 13, 4520, su *https://doi.org/10.3390/rs13224520.*

4. Altre aree di applicazione della Intelligenza Artificiale: l'analisi dei dati ambientali

Un ulteriore, importantissima area di applicazione di tecniche di Intelligenza Artificiale è relativa all'analisi integrata di banche dati ambientali e di altre banche dati di rilievo per la giurisdizione, alla ricerca di indicazioni utili per supportare le indagini contro il crimine ambientale, anche in integrazione con gli accertamenti svolti attraverso analisi di immagini terrestri.

Ad esempio, attualmente, esistono importanti banche dati nelle quali sono riversate, anche in base ad obblighi di legge, rilevanti informazioni pertinenti a tutte le fasi del ciclo dei rifiuti: produzione, trasporto, vigilanza sulle spedizioni, quadro dei gestori nazionale e locale, gestione del territorio, qualità ambientale[7]. È sentita la necessità di un sistema che permetta l'analisi integrata delle informazioni contenute in questi *database* unitamente ad altre informazioni complementari quali, ad esempio, dati catastali, informazioni sulle utenze, sulla movimentazione delle merci e prodotti.

Un prerequisito per l'analisi approfondita attraverso le tecniche di Intelligenza Artificiale di questi insiemi di dati è comunque il miglioramento della loro qualità, purtroppo spesso carente, ad esempio a causa di lacune, per ritardi nell'aggiornamento e disallineamenti nella gestione delle anagrafiche.

Anche la rivisitazione e la modernizzazione, eventualmente con il supporto di sistemi di Intelligenza Artificiale, delle banche dati a disposizione della giurisdizione, nella prospettiva di rendere disponibile un sistema informativo integrato in materia di criminalità ambientale dotati di strumenti di analisi ed estrazione adeguatamente selettive, rappresenta un obiettivo di assoluto valore nel contrasto alla criminalità ambientale.

5. Conclusioni

L'uso delle nuove tecnologie nel contrasto ai crimini ambientali rappresenta una opzione realistica ed irrinunciabile, che può portare alla disponibilità di un efficace sistema nazionale integrato di *Geospatial Intelligence* (GEOINT)[8] per il contrasto degli illeciti e del crimine ambientale.

---

7) Le banche dati sono gestite da una pluralità di soggetti (MiTE, SNPA, Sistema Camerale, comuni ed aree metropolitane).

8) Per GEOINT si intende un sistema in grado di associare ad "oggetti" collocati sul territorio e georeferenziati, eventualmente identificati con tecniche di osservazione terrestre, informazioni pertinenti estratte da sistemi informativi e *database*, allo scopo di associarli ad "attributi" che ne facilitano la "qualificazione". Importanti premesse per lo sviluppo di un sistema di GEOINT nazionale relativo ai rifiuti sono l'attuazione del REN - Registro elettronico nazionale per la tracciabilità dei rifiuti istituito dalla legge 11 febbraio 2019 n. 12, nonché il repertorio nazionale

Devono essere però considerate alcune fondamentali *condizioni al contorno*:

– la creazione di un contesto normativo adeguato ad accogliere l'innovazione tecnologica in modo robusto, promuovendone o quantomeno parificandone l'uso rispetto alle tecniche tradizionali, tanto in campo amministrativo che giurisdizionale;

– la modernizzazione delle infrastrutture informative esistenti per renderle idonee all'applicazione di tecniche di intelligenza artificiale;

– lo sviluppo di infrastrutture di supporto e applicazioni software e hardware realmente orientate alle caratteristiche ed esigenze dell'utenza, già nella fase della loro progettazione, attraverso un approccio integrato, con un contributo diretto dei futuri utenti, che testimoni e garantisca il rispetto, in particolare, delle specificità della giurisdizione e delle varie aree della protezione dell'ambiente;

– la disponibilità di risorse umane adeguate, sia per numero che per qualificazione,

e, infine:

– l'adozione di politiche adeguate alla conversione della pubblica amministrazione dall'approccio tradizionale a tecniche moderne più efficaci, uscendo dall'attuale confort *zone* per affrontare, attraverso una logica di riconversione tanto culturale quanto operativa, il percorso che prevede l'inserimento, tra i normali mezzi di lavoro, delle nuove tecnologie.

L'occasione per gli sviluppi tecnologici, organizzativi e procedurali solo parzialmente qui descritti è rappresentata dalla implementazione del Piano Nazionale di Ripresa e Resilienza (PNRR), che prevede cospicui investimenti per la modernizzazione della Pubblica Amministrazione e, in particolare, della Giustizia. Inoltre il PNRR prevede lo sviluppo di un *Sistema Avanzato di Monitoraggio Integrato del Territorio*[9], destinato ad alimentare anche la fase di prevenzione e repressione degli illeciti ambientali rilevabili con tecniche di osservazione terrestre (satelliti, aerei, droni) ed interpretati con tecniche di Gospatial Intelligence ed Intelligenza Artificiale.

La Fondazione Vittorio Occorsio ha affrontato in modo sistematico i temi qui descritti, attraverso uno specifico gruppo di lavoro relativo alle

dei dati territoriali, previsto dall'art. 59 del Codice dell'amministrazione digitale (D.lgs. n. 82/2005) e dal d.lgs. 19 agosto 2005, n. 195.

9) Si veda 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), che si propone appunto 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.

applicazioni dell'Intelligenza Artificiale e alle nuove tecnologie nella giurisdizione penale in campo ambientale. Tale gruppo di lavoro ha prodotto uno studio, i cui risultati sono sintetizzati in un *Position Paper* adottato dalla Fondazione[10], a disposizione dei Decisori per la definizione delle azioni di modernizzazione del sistema della protezione ambientale e di contrasto ai crimini ambientali in Italia.

10) Si veda: *Position Paper* redatto dal IV Gruppo di lavoro sull'Intelligenza Artificiale e giurisdizione penale - Reati in materia ambientale, coordinato dal dott. Pasquale Fimiani e dal dott. Antonello Arditurro, Roma, 19 novembre 2021, in *fondazioneoccorsio.it*.

L'impatto della digitalizzazione nelle attività investigative in materia ambientale

di Massimiliano Corsano, con l'ausilio di Massimo Planera*

1. Premessa

Il termine intelligenza artificiale (di seguito IA) indica una famiglia di tecnologie in grado di apportare una vasta gamma di benefici economici e sociali in tutto lo spettro delle attività industriali e sociali. L'uso dell'intelligenza artificiale, garantendo un miglioramento delle previsioni, l'ottimizzazione delle operazioni e dell'assegnazione delle risorse e la personalizzazione dell'erogazione di servizi, può infatti contribuire al conseguimento di risultati vantaggiosi dal punto di vista sociale e ambientale nonché fornire vantaggi competitivi fondamentali alle imprese e all'economia europea. Tale azione è particolarmente necessaria in settori ad alto impatto, tra i quali figurano quelli dei cambiamenti climatici, dell'ambiente e della sanità, il settore pubblico, la finanza, la mobilità, gli affari interni e l'agricoltura. Tuttavia gli stessi elementi e le stesse tecniche che alimentano i benefici socio-economici dell'IA possono altresì comportare nuovi rischi o conseguenze negative per le persone fisiche o la società ed è pertanto necessario delineare un "*recinto operativo*" all'interno del quale far rientrare l'utilizzo delle tecnologie più avanzate in materia di contrasto alla criminalità ambientale.

Si può trarre una definizione di IA nella "*Carta etica europea sull'utilizzo dell'Intelligenza Artificiale nei sistemi giudiziari*" adottata nel dicembre 2018 dalla CEPEJ: «*Insieme di metodi scientifici, teorie e tecniche finalizzate a riprodurre mediante le macchine le capacità cognitive degli esseri umani. Si distingue tra intelligenze artificiali "forti" (capaci di contestualizzare problemi specializzati di varia natura in maniera completamente autonoma) e intelligenze artificiali "deboli" o "moderate" (alte prestazioni nel loro ambito di addestramento*)».

La Carta individua cinque principi fondamentali cui attenersi nello sviluppo e utilizzo dell'I.A. nei sistemi giudiziari:

1) *principio del rispetto dei diritti fondamentali*: assicurare l'elaborazione e l'attuazione di strumenti e servizi di intelligenza artificiale che siano compatibili con i diritti fondamentali;

(*) Ten. Col. Massimiliano Corsano, Comandante del Reparto Operativo del Comando Carabinieri per la Tutela Ambientale e la Transizione Ecologica; Ten. Col. Massimo Planera, Comandante del Nucleo Operativo Centrale e Cooperazione Internazionale dell'Arma dei Carabinieri.

2) *principio di non-discriminazione*: prevenire specificamente lo sviluppo o l'intensificazione di discriminazioni tra persone o gruppi di persone

3) *principio di qualità e sicurezza*: in ordine al trattamento di decisioni e dati giudiziari, utilizzare fonti certificate e dati intangibili con modelli elaborati multidisciplinarmente, in un ambiente tecnologico sicuro;

4) *principio di trasparenza, imparzialità ed equità*: rendere le metodologie di trattamento dei dati accessibili e comprensibili, autorizzare verifiche esterne;

5) *principio "del controllo da parte dell'utilizzatore"*: precludere un approccio prescrittivo e assicurare che gli utilizzatori siano attori informati e abbiano il controllo delle loro scelte,

e classifica i possibili utilizzi della stessa I.A. in tre diverse categorie:

– da incoraggiare (vi rientrano: la valorizzazione del patrimonio giurisprudenziale; la creazione di nuovi strumenti strategici per migliorare l'efficienza della giustizia);

– da utilizzare con notevoli precauzioni metodologiche (comprendente, ad esempio, l'utilizzo nelle indagini al fine di prevedere ed individuare i luoghi in cui verranno o vengono commessi i reati);

– da esaminare al termine di supplementari studi o con le più estreme riserve (tra questi: la profilazione degli operatori di diritto, l'utilizzo di algoritmi in materia penale al fine di profilare le persone, estrazione di una «norma» basata sull'insieme delle decisioni ovvero elaborazione di una regola vincolante di decisione fondata sull'analisi dei precedenti).

L'esigenza di disciplinare il ricorso all'I.A. nei processi decisionali che coinvolgono soggetti giuridici viene avvertita anche dal legislatore nazionale che, con l'art. 8 del d.lgs. n. 51/2018, proibisce "*decisioni basate unicamente su un trattamento automatizzato, compresa la profilazione, che producono effetti negativi nei confronti dell'interessato, salvo che siano autorizzate dal diritto dell'Unione europea o da specifiche disposizioni di legge*. *Fermo il divieto di cui all'articolo 21 della Carta dei diritti fondamentali dell'Unione europea, è vietata la profilazione finalizzata alla discriminazione di persone fisiche sulla base di categorie particolari di dati personali di cui all'articolo 9 del regolamento UE*"[1].

Il 6 ottobre 2021, il Parlamento europeo ha adottato la risoluzione "*sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale*". La Risoluzione, particolarmente articolata, affronta i principali nodi problematici del rapporto tra

1) Sulla ricostruzione del quadro normativo cfr. Ziroldi, *Intelligenza artificiale e processo penale tra norme, prassi e prospettive*, in *questionegiustizia.it*, 18 ottobre 2019.

Intelligenza Artificiale e diritto penale auspicando, tra l'altro, la "*spiegabilità, la trasparenza, la tracciabilità e la verifica degli algoritmi… anche al fine di garantire che i risultati generati dagli algoritmi di IA possano essere resi intelligibili per gli utenti e coloro che sono soggetti a tali sistemi, e che vi sia trasparenza riguardo ai dati di base e alle modalità con cui il sistema è giunto a una certa conclusione*"[2].

Dall'analisi delle diverse tipologie di provvedimenti adottati, a livello sia nazionale, sia europeo, emerge, dunque, un'elevata aspettativa nei confronti dell'intelligenza artificiale riconosciuta come fattore di sviluppo anche in ambito giudiziario, ma con specifici profili controversi correlati ad alcuni usi della stessa I.A., potenzialmente discriminatori e alla capacità di garantire la necessaria trasparenza e intellegibilità nella ricostruzione del percorso algoritmico utilizzato dai sistemi per giungere alle conclusioni proposte.

L'aspetto della spiegabilità e della trasparenza degli algoritmi appare ancora più centrale nelle ipotesi di applicazione dell'I.A. al settore del diritto penale, sia processuale, sia sostanziale, dove sono in gioco i diritti fondamentali dell'indagato/imputato e della parte offesa, e dove, paradossalmente, il ricorso all'I.A. presenta peculiari suggestioni nella prospettiva di evitare ingiustificate disparità di trattamento o che possono apparire tali dal punto di vista del cittadino che entra nel meccanismo giudiziario.

Innanzitutto, quando parliamo di IA non dobbiamo necessariamente pensare ad un umanoide simile in tutto e per tutto all'essere umano: "*Poco, oltre alla speculazione e a un modo di pensare ingenuo, collega il lavoro odierno nel campo dell'IA ai misteriosi meccanismi della mente umana; in realtà, almeno a questo stadio, si tratta di una disciplina ingegneristica con relazioni più che altro metaforiche e di 'ispirazione' con gli organismi biologici*"[3], tanto più che l'intelligenza, intesa come quella degli esseri umani, prima ancora che delle macchine, per quanto sia oggetto di numerosissimi studi di psicologi, biologi e neuroscienziati, costituisce ancora un concetto indeterminato.

Per questo e per altri motivi talora i ricercatori di IA preferiscono parlare più che di intelligenza, di razionalità, laddove per "razionalità" si intende la capacità di scegliere la migliore azione da intraprendere per conseguire un determinato obiettivo alla luce di alcuni criteri di ottimizzazione delle risorse a disposizione.

2) Cfr. Martorana, *Intelligenza Artificiale e diritto penale, la risoluzione del Parlamento europeo*, in *altalex.com*, 12 novembre 2021.
3) Cfr. Kaplan, *Intelligenza artificiale*, Luiss University Press, 2018, p. 41.

2. IA e attività di *law enforcement*

Un sistema di IA perviene ad una scelta razionale percependo tramite sensori l'ambiente in cui è immerso e, dunque, raccogliendo e interpretando dati, ragionando su ciò che viene percepito o elaborando le informazioni desunte dai dati, decidendo quale sia l'azione migliore e agendo di conseguenza attraverso i suoi attuatori, eventualmente producendo una modifica del proprio ambiente.

Per meglio comprendere questa descrizione della razionalità dei sistemi di IA occorre altresì considerare che:

– i sensori potrebbero essere fotocamere, microfoni, una tastiera, un sito Internet o altri sistemi di immissione dati, nonché sensori di quantità fisiche (ad esempio, sensori di temperatura, di pressione, di distanza, di forza/coppia o sensori tattili);

– i dati acquisiti tramite i sensori sono dati digitali, di cui oggi vi è un'immensa disponibilità. A proposito dei dati, va sottolineato che la qualità del risultato finale dipende, in larga misura, proprio dalla correttezza logica e dalla completezza dei dati raccolti; per contro, se i dati utilizzati per alimentare o addestrare il sistema di IA sono distorti, nel senso che non sono sufficientemente equilibrati o inclusivi, il sistema non sarà in grado di generalizzare in maniera corretta e potrebbe adottare decisioni inique che possono favorire alcuni gruppi rispetto ad altri;

– il ragionamento o l'elaborazione delle informazioni è un processo operato attraverso un algoritmo che acquisisce come input i suddetti dati per poi proporre un'azione da intraprendere alla luce dell'obiettivo da raggiungere;

– infine, il sistema di IA esegue l'azione prescelta tramite gli attuatori a sua disposizione, che possono essere sia software, sia elementi fisici (ad esempio, bracci articolati, ruote automatiche), quest'ultimi capaci di intervenire, modificandolo, sull'ambiente circostante.

Oggi si riconosce unanimemente che i progressi compiuti dall'IA in tempi recenti sono stati consentiti dalla felice combinazione di due fattori: da un lato, l'aumento delle capacità computazionali, grazie alle quali oggi disponiamo di comput*er* sempre più veloci, potenti, con capacità di memoria (e, quindi, tra l'altro, di archiviazione dati) straordinariamente grandi; dall'altro lato, l'incremento di dati digitali raccolti anche grazie a sensori ad alta definizione e a basso costo, del tipo:

– *people-to-people*, provenienti dalla digitalizzazione di documenti o generati da ognuno di noi scattando foto, facendo video o inviando messag-

gi tramite le reti sociali o altri strumenti di messaggistica, come Whatsapp, Messenger, ecc.;

– *people-to-machine*, raccolti da istituzioni pubbliche o soggetti privati, inerenti ai cittadini o gli utenti, come dati fiscali, sanitari, ricerche sul web, transazioni commerciali, bancarie;

– *machine-to-machine*, generati automaticamente e indipendentemente dall'intervento di esseri umani, da dispositivi fisici, come ad esempio vari tipi di sensori, dispositivi di geo-localizzazione, werables, smart devices, tra di loro connessi attraverso il Web.

La combinazione di tali fattori ha consentito di elaborare e di diffondere su larga scala i sistemi di *machine learning* ovvero software che imparano autonomamente dall'ambiente esterno tramite i dati che immagazzinano ed elaborano e modificano le proprie prestazioni adattandole agli esiti del procedimento di apprendimento.

Nel documento di presentazione del Convegno annuale di esperti di Polizia, dedicato dall'OSCE nel 2019 proprio al tema "Artificial Intelligence and Law Enforcement", si legge: «*Nei loro sforzi per aumentare l'efficienza e l'efficacia e per stare al passo con le innovazioni tecnologiche, le autorità e le agenzie di law enforcement di tutto il mondo stanno esplorando sempre più i potenziali dell'IA per il loro lavoro. La crescente quantità di dati ottenuti e archiviati dalla polizia ha anche richiesto metodi e strumenti più sofisticati per la loro gestione e analisi, per l'identificazione di modelli (pattern), la previsione dei rischi e lo sviluppo di strategie per allocare le risorse umane e finanziarie dove sono maggiormente necessarie. Anche se l'uso dell'IA nel lavoro delle forze dell'ordine è un argomento relativamente nuovo, alcuni strumenti basati sull'intelligenza artificiale sono già stati testati e sono persino attivamente utilizzati dai servizi di polizia di diversi Paesi del mondo. Questi includono software di analisi di video e immagini, sistemi di riconoscimento facciale, di identificazione biometrica, droni autonomi e altri robot e strumenti di analisi predittiva per prevedere le "zone calde" del crimine o anche per identificare potenziali criminali futuri, in particolare i criminali ad elevata pericolosità*».

L'impiego di sistemi di IA nelle attività di *law enforcement* è, quindi, già una realtà, e se ne prevede una crescita ed intensificazione nei prossimi anni a vari livelli data la loro importanza strategica ed i preziosi risultati raggiungibili.

Circa i possibili impieghi dei sistemi di IA nel contrasto alla criminalità ambientale, sicuramente quelli più innovativi afferiscono alle attività di law enforcement rivolte alla prevenzione dei reati, con particolare attenzione allo specifico ambito denominato della "polizia predittiva".

3. Sistemi di intelligenza artificiale e polizia predittiva

Per "polizia predittiva" possiamo intendere l'insieme delle attività rivolte allo studio e all'applicazione di metodi statistici con l'obiettivo di "predire" chi potrà commettere un reato, o dove e quando potrà essere commesso un reato, al fine di prevenire la commissione dei reati stessi. La predizione si basa fondamentalmente su una rielaborazione attuariale di diversi tipi di dati, tra questi, quelli ritenuti di maggiore utilità per quanto afferisce alla criminalità ambientale riguardano sicuramente le notizie di reati precedentemente commessi, gli spostamenti (trasporti rifiuti, ndr) e le attività (distretti produttivi, ndr) di soggetti sospettati, ai luoghi, teatro di ricorrenti azioni criminali di tale tipologia e alle caratteristiche di questi luoghi, al periodo dell'anno o alle condizioni atmosferiche maggiormente connesse alla commissione di determinati reati: si pensi ad esempio al caso degli illeciti sversamenti di liquami in corpi idrici ricettori o nell'ambiente, che avvengono per lo più in periodi/giornate caratterizzate da piogge intense al fine di diluire con la pioggia le sostanze sversate o ancora agli incendi di rifiuti, che incrementano nei periodi estivi o comunque caratterizzati da caldo torrido al fine di rendere più difficile risalire a condotte dolose.

L'impiego di software basati sull'IA può consentire di fare un salto di qualità nelle attività di polizia predittiva, dal momento che è possibile l'acquisizione e la rielaborazione di una mole enorme di dati, scoprendo connessioni prima difficilmente individuabili dall'operatore umano.

I software di polizia predittiva, siano essi assistiti o meno da sistemi di IA, possono dividersi fondamentalmente in due categorie:

– quelli che, ispirandosi alle acquisizioni della criminologia ambientale, individuano le c.d. "zone calde" (*hotspots*), vale a dire i luoghi che costituiscono il possibile scenario dell'eventuale futura commissione di determinati reati;

– quelli che, ispirandosi invece all'idea del crime linking, seguono le serialità criminali di determinati soggetti (individuati o ancora da individuare), per prevedere dove e quando costoro commetteranno il prossimo reato.

Ad oggi sia gli uni che gli altri sistemi possono fornire adeguate previsioni solo in relazione a limitate, determinate categorie di reati e non in via generalizzata per tutti i reati, tuttavia la continua evoluzione tecnologica consente di poter ipotizzare alcuni scenari di impiago dell'IA anche per reati ambientali.

a) Sistemi di individuazione degli hotspots

Rientra in questa tipologia di sistemi il Risk Terrain Modeling (RTM): un algoritmo che, rielaborando quantità enormi di dati inerenti i fattori am-

bientali e spaziali favorenti la criminalità, potrebbe favorire la predizione della commissione di reati anche ambientali, il sistema è stato infatti elaborato dai ricercatori per sottoporre all'algoritmo RTM dati inerenti i fattori ambientali e spaziali più frequentemente connessi alla commissione di determinate tipologie di reati.

Ad oggi sono risultato particolarmente attendibili i risultati ottenuti nei monitoraggi effettuati sui reati di spaccio di sostanze stupefacenti in determinate aree urbane, laddove i dati inseriti afferiscono a presenza di luminarie stradali scarse o non funzionanti, vicinanza di locali notturni, di fermate di mezzi pubblici, di stazioni ferroviarie, di snodi di strade ad alta percorribilità, di bancomat, di compro-oro, di parcheggi scambiatori, infine, di scuole. Ciò ha consentito di elaborare una vera e propria "mappatura" di alcune grandi aree metropolitane al fine di individuare le "zone calde" dove più elevato risulta il rischio di spaccio di sostanze stupefacenti, con conseguenti benefici in termini di programmazione e attuazione di interventi di prevenzione della delinquenza connessa allo spaccio. In analogia si potrebbe procedere ipotizzando parametri per i delitti di inquinamento o disastro ambientale.

Parimenti finalizzato all'individuazione degli hotspots, ma testato in relazione ad un numero più elevato di reati (non solo quelli di spaccio) è anche un software, già in uso da alcuni anni negli Stati Uniti e nel Regno Unito, originariamente elaborato da alcuni ricercatori dell'UCLA (Università della California di Los Angeles) in collaborazione con la locale polizia, il *PredPol*, che sembrerebbe ispirarsi ad una analoga logica predittiva anche un dispositivo in uso presso la polizia italiana: il sistema informatico X-LAW. Tali software si basano su algoritmi capaci di rielaborare una mole enorme di dati estrapolati dalle denunce presentate. Tale rielaborazione consente di far emergere fattori ricorrenti o coincidenti o verificatisi con analoghe modalità. Ciò consente di tracciare una mappa del territorio dove vengono evidenziate le zone a più alto rischio fino a raggiungere il livello massimo in determinati orari, così consentendo, nelle zone e negli orari 'caldi', la predisposizione delle forze dell'ordine per impedire la commissione di tali reati e per cogliere in flagranza i potenziali autori degli stessi.

b) Sistemi di crime linking

L'idea del crime linking segue le serialità criminali di determinati soggetti, individuati o ancora da individuare, per prevedere dove e quando essi commetteranno il prossimo reato. Software ispirati all'idea del crime linking, e quindi all'individuazione delle persone, più che delle zone calde, sono stati elaborati, e sono in uso in Germania, in Inghilterra e negli Stati Uniti.

Questi software si basano sull'idea di fondo che alcune forme di cri-

minalità si manifesterebbero in un arco temporale e in una zona geografica molto circoscritti (c.d. near repeat crimes, o reati a ripetizione ravvicinata): ad esempio, la commissione di una rapina sembrerebbe essere associata ad un elevato rischio di commissione di una nuova rapina, da parte degli stessi autori e in una zona geografica assai prossima al luogo del primo delitto, entro le successive ore e, sia pur con un tasso di rischio decrescente, fino a tutto il mese successivo. Attraverso la raccolta e l'incrocio di una gran mole di dati, provenienti da varie fonti (ad esempio, immagini riprese da una telecamera o informazioni relative a precedenti analoghi reati), questi software cercano, infatti, di "profilare" il possibile autore della serie criminale e prevederne la prossima mossa. Tali sistemi, in ambito ambientale, potrebbero ad esempio essere utilizzati nella prevenzione di fenomenologie di criminalità ambientale diffusa afferenti, ad esempio agli abbandoni di rifiuti (sia urbani, sia speciali) o alla raccolta/trasporto/smaltimento illeciti di materiali ferrosi. Peraltro, i risultati forniti da questi software in alcuni casi potrebbero essere usati non solo a fini predittivi, ma anche per ricostruire la carriera criminale del soggetto profilato, vale a dire per avere una traccia di indagine da seguire per imputargli non solo l'ultimo reato commesso (in occasione del quale egli è stato individuato), ma anche i precedenti reati costituenti la serie criminale ricostruita grazie all'archiviazione e all'elaborazione dei dati.

4. I.A. e criminalità ambientale

Per "criminalità ambientale" si intende un fenomeno di preoccupante estensione in quanto dotato di una intrinseca trasversalità che coinvolge ambiti di interesse sempre più variegati oltre che soggetti o consorterie sempre più evoluti e, pertanto, fa riferimento all'insieme di condotte contrarie alla legge e direttamente lesive di un superiore diritto della persona che comprendono anche l'integrità fisica e psichica, oltre che la salvaguardia della qualità della vita. L'individuazione di un unico "*modus operandi*" nel contesto criminale legato all'ambiente non è di immediata, tuttavia le risultanze di analisi derivanti da anni di esperienza investigativa tendono a distinguere due diversi tipi di Criminalità Ambientale: quella diffusa e quella organizzata, laddove con la prima si può intendere una qualsiasi condotta occasionale che lede l'ambiente e che fa riferimento anche a condotte mono-soggettive, mentre la Criminalità Ambientale organizzata è tipizzata da un'area comune d'interesse criminale in cui le condotte delinquenziali si distinguono per la sistematicità e l'organizzazione di strutture e mezzi. In quest'ultimo ambito, si dovranno verificare gli interessi e la consistenza che frange di criminalità organizzata

di tipo mafioso ed imprese criminali pongono rispetto al settore ambientale laddove i reati commessi rappresentano non il fine bensì il mezzo attraverso il quale conseguire gli obiettivi criminali del sodalizio, motivo per cui il reato ambientale rappresenta un reato mezzo nelle condotte delittuose, in quanto la commissione di delitti contro l'ambiente costituisce il presupposto per il conseguimento di vantaggi economici ingiusti. La componente ambientale rappresenta un'opportunità economica appetibile per i più svariati interessi criminali, vieppiù alla luce delle difficoltà economiche derivanti dalla pandemia in atto, che potrebbero favorire oltremodo l'ingresso di capitali di provenienza illecita in attività imprenditoriali attive nel ciclo gestionale dei rifiuti e, più in generale, nel più vasto settore delle "*green, circular, bio economy*". Infatti se i cicli dei rifiuti e del cemento si configurano quali comuni denominatori "storici" del variegato cosmo delle attività illecite, altri settori che, negli ultimi anni, hanno attratto l'attenzione delle organizzazioni criminali sono quelli delle energie alternative, della decarbonizzazione e, più in generale, della sostenibilità, la cui diffusione è promossa per mezzo di programmi di sensibilizzazione e soprattutto di incentivazione.

In un così complesso e variegato contesto, l'utilizzo di sistemi di IA rappresenta certamente una necessità alla luce degli evidenti vantaggi anche in campo predittivo, dinanzi largamente trattati.

In tale ottica, si citano ad esempio l'applicazione del RENTRI[4] (Registro Elettronico Nazionale sulla Tracciabilità dei Rifiuti) che introduce un modello di gestione digitale per l'assolvimento di taluni adempimenti in materia di gestione dei rifiuti, oppure gli studi – condotti con il contributo del Comando Carabinieri per la Tutela Ambientale e la Transizione Ecologica – in materia di utilizzo di immagini iperspettrali per l'individuazione di forme di inquinamento nelle varie matrici ambientali, e ancora la disamina della possibilità di impiego delle *Blockchain* nel tracciamento dei rifiuti e le sperimentazioni per la classificazione automatizzata del rifiuto.

Un esempio particolarmente virtuoso ha peraltro visto la luce di recente: *Nature* ha infatti pubblicato la ricerca di un team multidisciplinare dell'Università del Texas (Austin) che ha messo a punto, grazie ad un algoritmo di machine-learning, un enzima in grado di 'smontare' le lunghe catene chimiche del PET (quello delle bottiglie ma anche di una grandissima quantità di imballaggi, fibre tessili e altri oggetti) nei mattoncini che le compongono (i monomeri). Il sistema è stato denominato FAST-PETasi (in inglese "Functional, Active, Stable and Tolerant PETase"), un catalizzatore naturale, un enzi-

4) Cfr. d.lgs. 3 settembre 2020 n. 116.

ma, una proteina prodotta da batteri e ingegnerizzata dai chimici americani in modo da po*ter* sciogliere (idrolizzare) il polietilene tereftalato (PET) nei suoi componenti: acido ftalico e glicole etilenico[5].

Dunque l'IA salverà il mondo?... non proprio…

A titolo meramente esemplificativo, infatti, si cita quanto sta accadendo ormai quotidianamente in tema di "sostenibilità". In un mercato finanziario che vede – sul fronte dei "fondi sostenibili" – un patrimonio globale di 2.770 miliardi di dollari, assume una funzione fondamentale lo *Scoring* dei rating ESG (Environmental, Social and Governance), effettuato attraverso sistemi algoritmici, al fine di indirizzare gli investimenti verso le aziende maggiormente virtuose. Ebbene i dati di analisi dimostrano come di fatto l'intelligenza umana stia prevalendo su quella artificiale, giacché sul mercato si stanno affermando professionisti che redigono Dichiarazioni Non Finanziarie - DNF[6] di comodo – i c.d. Bilanci di Sostenibilità – attraverso l'utilizzo sapiente di standard internazionali e parole chiave che ingannano i software così portando alla massimizzazione dei punteggi valutativi pur in assenza di reali politiche sostenibili.

Questo è solo uno dei molteplici esempi di come le IA rappresentino certamente un fondamentale ausilio all'operato umano anche nel settore del contrasto ai reati ambientali, ma debbano essere appunto catalogate come "ausilio" e non come sostituto dell'intelligenza umana, proprio per la più volte richiamata necessità di procedere sempre in via preliminare ad effettuare le necessarie verifiche metodologiche.

In conclusione, i sistemi di polizia predittiva sinteticamente descritti possono indubbiamente quindi apportare benefici nella prevenzione almeno di alcune tipologie di reati ambientali, anche se molte sono le perplessità che suscitano il loro utilizzo.

La scarsa regolamentazione a livello normativo del loro utilizzo fa sì che le condizioni e le modalità del loro utilizzo, nonché la valutazione e la valorizzazione dei loro risultati finiscono per essere affidate alla sola prassi, e quindi all'iniziativa, alla sensibilità, all'esperienza degli operatori di polizia.

Inoltre, come già anticipato il loro uso potrebbe implicare gravi attriti quanto meno con la tutela della privacy e con il divieto di discriminazione,

5) Cfr. Di Stefano, *L'intelligenza artificiale scende in campo per il riciclo (chimico) della plastica*, in *Economiacircolare.com*, 10 maggio 2022.

6) La Dichiarazione Non Finanziaria che gli Enti di Interesse Pubblico definiti dall'art. 16 del d.lgs. 39/2010 devono obbligatoriamente redigere ai sensi del d.lgs. 254/2016. A tal proposito, appare ormai imminente l'adozione di modiche normative in ambito europeo volte a modificare la regolamentazione in materia di bilancio (Direttiva 2013/34/EU) e di NFD (Direttiva 2014/95/EU) e dunque ad ampliare notevolmente la platea di soggetti obbligati alla redazione della DNF ed infatti il 21 aprile 2021 è stata pubblicata la proposta di direttiva europea c.d. *Corporate Sustainability Directive* (CSDR) n. 2021/0104.

nella misura in cui, ad esempio, identifichino fattori di pericolosità connessi a determinate caratteristiche etniche, o religiose o sociali.

Si tratta, poi, di sistemi che in una certa misura si auto-alimentano coi dati prodotti dal loro stesso utilizzo, col rischio di innescare circoli viziosi: se, ad esempio, un software predittivo individua una determinata "zona calda", i controlli e i pattugliamenti delle Forze di Polizia in quella zona si intensificheranno, con inevitabile conseguente crescita del tasso dei reati rilevati dalla polizia in quella zona, che diventerà, quindi, ancora più "calda", mentre altre zone, originariamente non ricondotte nelle "zone calde", e quindi non presidiate, rischiano di rimanere, o di diventare, per anni zone franche per la commissione di reati.

Infine, non si deve trascurare il fatto che la maggior parte di questi software sono coperti da brevetti depositati da aziende private, i cui detentori sono, giustamente, *gelosi* dei relativi segreti industriali e commerciali, sicché non si può disporre di una piena comprensione dei meccanismi del loro funzionamento, con evidente pregiudizio delle esigenze di trasparenza e di verificazione indipendente della qualità e affidabilità dei risultati da essi prodotti.

Un cambiamento è dunque in atto e avrà un imponente impatto anche nel settore del contrasto alla criminalità ambientale, il compito degli operatori è quello di guidare il percorso verso i nuovi modelli operativi evitando pericolose deviazioni, tenendo sempre a mente che "*la misura dell'intelligenza è la capacità di cambiare*" (Albert Einstein).

Bibliografia

Per la parte tecnico-scientifica del testo è stata utilizzata la bibliografia citata nelle note del documento ed è stato tratto spunto dalle seguenti opere/articoli:

– Basile F., *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *penalecontemporaneo.it*, 29 settembre 2019;

– Ferrari V., *Note socio-giuridiche introduttive per una discussione su diritto, intelligenza artificiale e big data*, Franco Angeli, 2020;

– Parodi C. - Sellaroli V., *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco*, in *penalecontemporaneo.it*, 6 giugno 2019;

– Patscot R. - Bisogni M., *Intelligenza artificiale e dati giudiziari: verso una "iurisfera" digitale del procedimento penale (telematico)?*, in *ilprocessotelematico.it*, 17 marzo 2022;

– Rulli E., *Giustizia predittiva, intelligenza artificiale e modelli probabilistici. Chi ha paura degli algoritmi?*, in *Analisi giuridica dell'economia*, 2018, II, 538.