

**La scienza delle previsioni
al servizio dell'investigazione e della prevenzione:
il punto di vista dell'Avvocato-Investigatore**

SOMMARIO: 1. Introduzione: oggetto, obiettivo e metodo. - 2. Cenni sulla scienza delle previsioni. - 3. Gli algoritmi predittivi della pericolosità criminale: problemi di costituzionalità. - 4. Cornice UE. - 5. Investigazione e prevenzione: a) *Keycrime*; b) *Social Network Analysis*; c) Investigazioni difensive preventive. - 6. Spunti per un metodo investigativo difensivo.

1. Introduzione: oggetto, obiettivo e metodo. - Il contributo¹ ha l'obiettivo di avviare, in campo criminologico, un dibattito sulla scienza delle previsioni - che si è evoluta assimilando dati, modelli matematici e intelligenza artificiale (di seguito IA) - in relazione alle investigazioni, nonché alla polizia di predizione.

Non esiste un confine alle applicazioni che possiamo immaginare: occorre essere consapevoli che stiamo entrando in una nuova era, dove riuscire a prevedere il futuro sarà una pratica costante a partire dai fenomeni sociali per arrivare ai bisogni di ogni singolo individuo.

In punto di diritto è necessario verificare se, e in che termini, sia costituzionale l'impiego dei *risk assessment tools*, ossia degli strumenti computazionali in grado di calcolare il rischio che un prevenuto si sottragga al processo o commetta dei reati, potendo il loro "responso" costituire eventuale presupposto per l'applicazione di una qualche misura.

Criterio guida sono i canoni UE dell'impegno per una IA affidabile e del divieto di decisioni basate unicamente su un trattamento automatizzato.

¹ L'A. ha presentato oralmente questo articolo nella Sessione A1 del XXXIII Congresso Nazionale della Società Italiana di Criminologia (Modena, 24-26 ottobre 2019).

Sul versante operativo, vengono approfonditi il programma *Keycrime*, creato all'interno della Questura di Milano, il ruolo della *Social Network Analysis* e il trascurato privilegio delle investigazioni difensive preventive di cui all'art. 391 *nonies* del codice di procedura penale italiano.

Utilizzando un metodo problematico e interdisciplinare, si perviene a formulare qualche idea circa l'elaborazione di un metodo investigativo difensivo.

2. Cenni sulla scienza delle previsioni². - Oggi siamo costantemente aiutati da un esercito di algoritmi³ che prevede quello che ci succede intorno, i nostri bisogni e le nostre prossime mosse; i dati passati alimentano le analisi del presente e disegnano le mappe del nostro futuro: ormai siamo abituati ad essere previsti.

I dati e le informazioni non equivalgono a nuova conoscenza: ciò che li trasforma in potere predittivo – setacciandoli, filtrandoli e conferendo un senso – sono gli **algoritmi**, un insieme di regole che definiscono con precisione una sequenza di operazioni. Gli algoritmi possono eseguire operazioni di calcolo, elaborazione dati e ragionamento automatico, e sono fondamentali per il modo in cui i computer eseguono istruzioni specifiche.

Partire da una maggiore **consapevolezza** è la chiave per essere sicuri che questo potere predittivo non venga usato per manipolarci o controllarci; infatti, ogni informazione sulla nostra vita è diventata un dato digitale che può essere conservato e analizzato, consentendo di mettere la società, in ogni suo più piccolo aspetto, al microscopio.

Particolare interesse destano i *neural networks*, algoritmi di *machine learning* basati su un modello semplificato del cervello umano. Un insieme di unità (neuroni) riceve un input ed esegue calcoli semplici trasferiti al successivo livello di unità. Il livello finale rappresenta la

² Cfr. A. VESPIGNANI, *L'algoritmo e l'oracolo. Come la scienza predice il futuro e ci aiuta a cambiarlo*, il Saggiatore, 2019.

³ Sugli algoritmi predittivi e, più in generale, sulla giustizia predittiva, v. L. VIOLA, *Giustizia predittiva*, in www.treccani.it; C. CASTELLI, D. PIANA, *Giustizia predittiva. La qualità della giustizia in due tempi*, in www.questionegiustizia.it; E. QUARTA, *Giustizia e predizione: l'algoritmo che legge il futuro*, in www.giustiziainsieme.it; A. SCOSCIA, *Giustizia predittiva: un algoritmo a supporto delle decisioni*, in www.fondazionebassetti.org.

risposta dell'algorithm⁴. Il **problema**, tuttavia, è che le reti neurali non sono in grado di esplicitare il perché dei loro risultati, con tutte le conseguenze che ne derivano in termini di **affidabilità**.

Occorre, inoltre, porsi un **problema di etica** delle previsioni, poiché stiamo entrando in un'era in cui dati e algoritmi permettono la costruzione e l'analisi di scenari che definiscono delle vere e proprie mappe del futuro. Peraltro, richiedendo le previsioni enormi infrastrutture, si può intravedere un mondo a due velocità, dove le diseguaglianze socio-economiche si riflettono anche in una **diseguaglianza di intelligenza predittiva**⁵.

Dati e algoritmi rappresentano una rivoluzione scientifica della stessa portata della comprensione del mondo subatomico, ma la ricerca di punta avviene all'interno di **compagnie private** che producono non solo la scienza ma anche l'equivalente del plutonio, ovvero i dati.

Se anni fa vi era l'enunciato secondo cui le previsioni non si applicano al singolo individuo, oggi è meno semplice sostenere che non è o non sarà possibile fare **predizioni individuali**.

Ad esempio, nel 2013 Chaoming Song, ricercatore della Miami University, mostrò un algoritmo che, analizzando le tracce GPS di telefonia cellulare di un individuo, riusciva a prevedere con una precisione media del 93% dove quella persona si trovasse in qualsiasi momento di qualsiasi giorno. Alle stesse piattaforme di condivisione consegniamo pensieri, preferenze, amicizie, nonché la mappa delle nostre relazioni sociali: depositi aperti al pubblico, grazie ai quali è possibile esaminare milioni di persone.

Ancora: è stato sviluppato un algoritmo di *machine learning* per identificare e prevedere un principio di depressione dai post pubblicati su Instagram da parte di pazienti con disturbi

⁴ Sulle reti neurali, v. G. COSTABILE, *Prevedere i crimini: l'intelligenza artificiale per le investigazioni*, in www.agendadigitale.eu.

⁵ "... si tratta di gestire con consapevolezza questa fase, prima di tutto comprendendola. Per farlo abbiamo bisogno di sapere cosa stia realmente accadendo nei laboratori di ricerca pubblici e, soprattutto, privati di tutto il mondo. Queste conoscenze sono in gran parte possedute da pochissime aziende a livello mondiale, circostanza che pone un serio problema di accesso e di condivisione, poiché potrebbe aprire un solco incolmabile tra chi può utilizzare e programmare l'intelligenza artificiale e chi no, forse addirittura andando a creare due diversi tipi di esseri umani. Un problema che diventa politico e costituisce un punto di svolta del XXI secolo, imponendo di approfondire le conseguenze di tali processi sugli stati" (così M. CALIGIURI, *Intelligenza artificiale e ordine mondiale*, in *Gnosis - Riv. It. Intelligenza*, 1/2018, 58).

psichiatrici: lo studio apre la possibilità alla predizione in tempo reale dell'inizio di problemi di tipo depressivo, monitorando l'attività nei *social* dei pazienti.

Più in particolare, gli **ambiti** all'interno dei quali la rivoluzione tecnologica potrebbe più significativamente impattare con le pretese di tutela dei beni giuridici, affidate al diritto penale, sono fondamentalmente tre: 1) le attività di *law enforcement* e di polizia predittiva - dove i sistemi di IA possono fornire un importante contributo per prevenire la commissione di reati -, compresa la valutazione di pericolosità criminale affidata ad algoritmi predittivi, capaci di rielaborare quantità enormi di dati al fine di far emergere correlazioni che consentano di profilare una persona e prevederne i successivi comportamenti, anche di rilevanza penale; 2) il possibile impiego di algoritmi decisionali per risolvere procedimenti penali, così da operare una sorta di affiancamento del giudice-uomo col giudice-macchina; 3) le possibili ipotesi di coinvolgimento - come strumento, come autore o come vittima - di un sistema di IA nella commissione di un reato. Soltanto il primo punto è oggetto di questo studio.

3. Gli algoritmi predittivi della pericolosità criminale: problemi di costituzionalità⁶. - È probabile che un soggetto, avente determinate caratteristiche, possa in futuro commettere un (nuovo) delitto?

Occorre porsi questa domanda quando si tratta, ad esempio, di applicare una misura di sicurezza, una misura cautelare, una misura di prevenzione, o anche di disporre la sospensione del procedimento con messa alla prova, la sospensione condizionale della pena o l'affidamento in prova al servizio sociale.

Negli Stati Uniti già da anni sono in fase di diffusione algoritmi predittivi della pericolosità criminale (*risk assessment tools*). Essi sono adoperati per decidere se un individuo, nelle more

⁶ Cfr. F. BASILE, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Diritto Penale e Uomo*, 29 settembre 2019, 16.

Studio Avv. Simone Ferrari

Criminologo e Dottore di ricerca in Diritto Penale

della celebrazione del processo, possa essere rilasciato dietro il pagamento di una cauzione (*bail*), per misurare il rischio di recidiva del condannato⁷, ecc.

Lo Stato del New Jersey, nell'intento di riformare l'istituto del *parole*⁸, ha introdotto un sistema algoritmico di valutazione della pericolosità criminale, denominato *Public Safety Assessment - PSA*, col proposito di fornire ai giudici, impegnati a formulare una prognosi criminale, indicazioni scientifiche ed imparziali in tempi rapidi.

Da quando il PSA è stato adottato, nello Stato del New Jersey il numero delle persone rilasciate su *parole* è aumentato; soprattutto è aumentato il numero delle persone rilasciate senza il pagamento di una cauzione: l'algoritmo sembra, pertanto, aver favorito i soggetti non pericolosi e non abienti.

Un altro algoritmo predittivo è quello di **COMPAS** - *Correctional Offender Management Profiling for Alternative Sanctions*.

Talune perplessità nei confronti di COMPAS hanno riguardato il suo possibile utilizzo in sede di *sentencing*, fase del procedimento penale in cui si determina il *quantum* di pena. Le critiche sono segnatamente emerse in relazione al **caso Loomis**, dal nome di un imputato che aveva fatto ricorso alla Corte Suprema del Wisconsin per contestare l'entità della pena che gli era stata inflitta dalla Corte locale la quale, in fase commisurativa, si era per l'appunto avvalsa di COMPAS: l'algoritmo predittivo veniva criticato dal ricorrente per la sua predisposizione a seguire pregiudizi basati sul genere e sulla razza, nonché per il difetto di trasparenza relativo al suo meccanismo di funzionamento.

La Corte Suprema del Wisconsin, sollecitata da tali rilievi, ha formulato un *warning* in relazione al futuro uso di COMPAS, mettendo in evidenza: 1) la sua natura di prodotto coperto da segreto industriale, che impedisce la divulgazione di informazioni relative al metodo di

⁷ Cfr. I. GITTARDI, *Il database di casi giudiziari del Center for Science and Law*, in *Diritto Penale e Uomo*, 19 giugno 2019.

⁸ Il *Parole Board* è un organo consultivo di natura amministrativa, composto da giudici, psichiatri, criminologi e sociologi. Esso ha il compito di osservare il comportamento dei condannati a pena detentiva per valutare se possono ritenersi risocializzati. In caso affermativo, viene data comunicazione all'*Home Secretary* che può emettere ordine di scarcerazione, sempre che il condannato abbia già scontato una parte della pena (S. VINCIGUERRA, *Glossario*, in *Diritto penale inglese comparato. I principi*, Cedam, 2002, 19).

Studio Avv. Simone Ferrari

Criminologo e Dottore di ricerca in Diritto Penale

funzionamento; 2) il fatto che le valutazioni sono effettuate su base collettiva, di gruppo, e non individuale; 3) il rischio di una sovrastima del rischio di commissione di reati a carico di talune minoranze etniche. Ciò nondimeno, nel caso di specie, la Corte Suprema ha respinto il ricorso del sig. Loomis, sulla scorta della considerazione che le valutazioni di COMPAS non erano state decisive, in quanto erano state pur sempre sottoposte al controllo e alla validazione di un giudice umano.

Orbene, i sostenitori dell'impiego degli algoritmi predittivi ritengono che questi software, grazie all'elaborazione di *big data* e all'apprendimento automatico, rendono le valutazioni di pericolosità criminale più accurate e maggiormente esenti dal rischio di risentire di condizionamenti culturali.

Per contro, sono state sollevate riserve in ordine all'effettiva validità predittiva, all'imparzialità, all'esigenza di una valutazione individualizzata della pericolosità criminale, alla trasparenza, alla deresponsabilizzazione dei giudicanti.

Il nostro **problema** è di comprendere se in Italia le valutazioni prognostiche della pericolosità criminale possano essere affidate a specifici algoritmi.

Dal punto di vista della **Costituzione italiana**, va rilevato che se la decisione sulla pericolosità fosse totalmente rimessa alle elaborazioni di un programma, si profilerebbe un inevitabile contrasto con gli artt. 25 e 111 Cost., laddove richiamano espressamente la figura del "giudice" (umano). Del resto, per garantire un intervento effettivo dell'uomo, la decisione non può basarsi esclusivamente sul responso di un meccanismo automatizzato: accanto all'obbligo di un intervento umano, va ritenuta sussistente anche una regola di valutazione in forza della quale l'output prodotto dall'IA è da considerare solamente come un mero indizio.

In campo amministrativo si è peraltro di recente affermato che la decisione amministrativa automatizzata, di per sé legittima, impone al giudice di valutare in primo luogo la correttezza del processo informatico in tutte le sue componenti: dalla sua costruzione, all'inserimento dei dati, alla loro validità, alla loro gestione; da qui si conferma la necessità di assicurare che quel processo, a livello amministrativo, avvenga in maniera trasparente, attraverso la conoscibilità dei dati immessi e dell'algoritmo medesimo. In secondo luogo, il giudice deve poter sindacare

E avv.simoneferrari@gmail.com
P simoneferrari@pec.it
T +39 349 5186371

Piazza Vittorio Emanuele II, 3/B
10024 | Moncalieri
(Torino)

la stessa logicità e ragionevolezza della decisione amministrativa robotizzata, ovvero della “regola” che governa l’algoritmo⁹.

4. Cornice UE¹⁰. - In Europa, gli algoritmi predittivi della pericolosità criminale (e, più in generale, gli *automated decision systems*), non hanno avuto accesso nelle aule penali, anche perché vi è oggi l’art. 22 **RGPD**.

Tale articolo stabilisce, infatti, che l’interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

Al fine di verificare segnatamente gli spazi applicativi dei *risk assessment tools* nel procedimento penale, lo strumento rilevante è la **Direttiva 2016/680/UE** (relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati)¹¹.

La norma di riferimento è quella dell’art. 11 sul processo decisionale automatizzato relativo alle persone fisiche, ove si stabilisce che gli Stati membri dispongono che una decisione basata unicamente su un trattamento automatizzato, compresa la profilazione, che produca effetti giuridici negativi o incida significativamente sull’interessato sia vietata, salvo che sia autorizzata dal diritto dell’Unione o dello Stato membro cui è soggetto il titolare del trattamento e che preveda garanzie adeguate per i diritti e le libertà dell’interessato, almeno il diritto di ottenere l’intervento umano da parte del titolare del trattamento.

⁹ Cons. Stato, Sez. VI, n. 2270/2019.

¹⁰ Cfr. F. BASILE, *Intelligenza artificiale e diritto penale*, cit., 22; M. GIALUZ, *Quando la giustizia penale incontra l’intelligenza artificiale: luci e ombre dei risk assessment tools tra Stati Uniti ed Europa*, in *Diritto Penale Contemporaneo*, 12.

¹¹ Direttiva attuata con D.Lgs. n. 51/2018.

In altre parole e come già accennato, al fine di garantire un intervento effettivo dell'uomo, la decisione non può basarsi esclusivamente sull'output di un meccanismo automatizzato: accanto all'obbligo di un intervento umano deve sussistere una regola di valutazione in forza della quale l'output prodotto dall'IA va considerato come un mero indizio, sempre da corroborare con altri elementi di prova.

Ancora in ambito UE, occorre ricordare che la **Risoluzione del Parlamento europeo sulla robotica del 16 febbraio 2017** pone l'accento sul principio della trasparenza, nello specifico sul fatto che dovrebbe sempre essere possibile indicare la logica alla base di ogni decisione presa con l'ausilio dell'IA che possa avere un impatto rilevante sulla vita di una o più persone; ritiene che debba sempre essere possibile ricondurre i calcoli di un sistema di IA a una forma comprensibile per l'uomo; reputa che i robot avanzati dovrebbero essere dotati di una "scatola nera" che registri i dati su ogni operazione effettuata dalla macchina, compresi i passaggi logici che hanno contribuito alle sue decisioni.

Sul versante della **Convenzione Europea dei Diritti dell'Uomo**, laddove si prospetti un utilizzo dei *risk assessment tools* nella materia della libertà personale, vengono in gioco le garanzie dell'art. 5 e, in particolare, il diritto all'accesso al giudice, nelle sue due forme contemplate dal par. 3 (diritto di essere tradotti al più presto dinanzi a un giudice) e dal par. 4 (diritto di presentare un ricorso a un tribunale, affinché decida entro un breve termine sulla legittimità della detenzione e ne ordini la scarcerazione se la detenzione è illegittima), nonché l'obbligo di motivazione.

Infine, talune indicazioni provengono dalla Commissione europea per l'efficienza della giustizia (Cepej) del Consiglio d'Europa, con la **Carta etica europea** sull'uso dell'IA nei sistemi giudiziari e in ambiti connessi (3 dicembre 2018)¹².

La Cepej rileva che l'uso di strumenti e servizi di IA nei sistemi giudiziari è volto a migliorare l'efficienza e la qualità della giustizia, e merita di essere incoraggiato. Tuttavia, ciò deve avvenire in modo responsabile, nel rispetto dei diritti fondamentali sanciti dalla CEDU e

¹² La Carta etica fissa cinque principi: 1) quando gli strumenti di IA vengono impiegati come ausilio nei processi, si deve assicurare che non violino il diritto di accesso al giudice e il diritto a un processo equo; 2) non discriminazione; 3) qualità e sicurezza; 4) trasparenza, imparzialità e correttezza; 5) *under user control*.

dalla Convenzione 28 gennaio 1981 del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, nonché degli altri principi fondamentali enunciati nella Carta¹³.

5. Investigazione e prevenzione: a) *Keycrime*¹⁴. - Per “polizia predittiva” si intende l'insieme delle attività rivolte allo studio e all'applicazione di metodi statistici con l'obiettivo di predire chi potrà commettere un reato, nonché dove e quando potrà essere commesso un reato, al fine di prevenirne la commissione.

La predizione si basa su una rielaborazione di diversi tipi di dati, fra cui quelli relativi a notizie di reati precedentemente commessi, alle attività di soggetti sospettati, ai luoghi di ricorrenti azioni criminali, al periodo dell'anno o alle condizioni atmosferiche; fra i dati utilizzati a questi fini, talora compaiono anche informazioni relative all'origine etnica, al livello di scolarizzazione, alle condizioni economiche, alle caratteristiche somatiche.

Più in dettaglio, i software di polizia predittiva possono dividersi in due categorie: 1) quelli che, ispirandosi alle acquisizioni della criminologia ambientale, individuano le c.d. “zone calde” (*hotspots*), vale a dire i luoghi che costituiscono il possibile teatro dell'eventuale futura consumazione di reati; 2) 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 realizzeranno il prossimo delitto.

Rientra nel primo tipo di sistemi il *Risk Terrain Modeling (RTM)*: un algoritmo che, rielaborando quantità enormi di dati inerenti ai fattori ambientali e spaziali favorevoli alla criminalità, sembrerebbe consentire la predizione della commissione di reati di spaccio di sostanze stupefacenti in determinate aree urbane (presenza di luminarie stradali scarse o non funzionanti, vicinanza di locali notturni, di fermate di mezzi pubblici, di stazioni ferroviarie, di

¹³ Sul punto v. C. BARBARO, *Cepej, adottata la prima Carta etica europea sull'uso dell'intelligenza artificiale (AI) nei sistemi giudiziari*, in www.questionegiustizia.it.

¹⁴ Cfr. C. PARODI, V. SELLAROLI, *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco*, in *Diritto Penale Contemporaneo*, 6/2019, 56; F. BASILE, *Intelligenza artificiale e diritto penale*, cit., 10; A. ZIROLDI, *Intelligenza artificiale e processo penale tra norme, prassi e prospettive*, in www.questionegiustizia.it.

Studio Avv. Simone Ferrari

Criminologo e Dottore di ricerca in Diritto Penale

snodi di strade ad alta percorribilità, di bancomat, di compro-oro, di parcheggi scambiatori, di scuole, ecc.)¹⁵.

Si rifà, invece, all'idea del *crime linking*, seguendo le serialità criminali di determinati soggetti, per prevedere dove e quando essi commetteranno il prossimo reato, il software *Keycrime*, originariamente elaborato presso la Questura di Milano.

Il limite del programma è appunto la sua utilizzabilità solo a fronte di condotte seriali. Decisive sono qualità e quantità di informazioni nonché tempestività e completezza della raccolta e dell'inserimento delle stesse.

“Capii ... che tutti quei dati e quei particolari che erano scritti sui fogli che noi poliziotti compilavamo a ogni fine turno, potevano e dovevano essere trasposti su un supporto informatico; così iniziai a creare un database in cui anche il minimo particolare aveva la propria casella. In tanti anni di immagazzinamento dati, quel database assunse proporzioni di un certo rilievo. Dunque, a questo punto, serviva un qualcosa che analizzasse i dati e li incrociasse tra loro per arrivare a trarre le prime conclusioni ... iniziai a mettere in campo tutte le conoscenze acquisite nel tempo fino a elaborare l'embrione di un algoritmo di analisi criminale, che poi sarebbe diventato un modello matematico ... riuscimmo, tramite l'individuazione della serialità legata ad un rapinatore, a individuare il luogo e il momento in cui avrebbe colpito di nuovo. Abbiamo collocato le volanti, nel lasso di tempo e nel luogo dove il programma aveva indicato potesse accadere la rapina successiva, ed abbiamo aspettato. In effetti la rapina avvenne ... Il funzionamento del programma è incredibilmente semplice nella sua complessità, ma alla base di tutto c'è sempre l'elemento umano. Quando avviene una rapina la squadra di *Keycrime* si mette subito al lavoro raccogliendo nell'immediato una serie di informazioni, attraverso un protocollo di intervento che mira a raccogliere, da chi ha subito il reato o ne è stato semplicemente testimone, una consistente mole di dati fondamentale per 'analizzare' l'evento ... In questo modo ... le informazioni, sommate all'analisi effettuata fotogramma per fotogramma sui filmati recuperati dagli impianti a circuito chiuso, vengono inserite all'interno dell'interfaccia grafica di *Keycrime*. Alla fine della procedura, l'algoritmo matematico

¹⁵ Parimenti, nel 2006 in California una squadra di matematici, antropologi, criminologi ed informatici ha iniziato a lavorare ad un algoritmo che elabora modelli statistici in grado di prevedere dove e quando avverrà un crimine; il software, *PredPol*, raccoglie informazioni dai casellari giudiziari e le incrocia con dati estrapolati dalle comunicazioni via radio delle pattuglie. L'algoritmo produce ogni giorno una lista delle 10 aree della città dove è più alta la probabilità che avvenga un reato: in queste zone la polizia esercita un'azione di dissuasione (cfr. www.predpol.com). In questa prospettiva, in Italia viene utilizzato il sistema informatico *X-LAW*.

creato da Mario Venturi elabora e incrocia tutti i dati: corporatura, abbigliamento, *modus operandi*, orari, luoghi e dà un risultato, proponendo al poliziotto una serie di eventi che sono potenzialmente collegabili con quello appena inserito. Questa procedura permette di collegare tra loro dei reati che altrimenti potrebbero rimanere fatti singoli e a sé stanti sui quali sarebbe difficile se non impossibile indagare. La serie criminale così isolata consente di avere capacità predittive con ottime probabilità di successo”¹⁶.

Peraltro, i risultati forniti da questo software possono 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 svelata grazie all’archiviazione e all’elaborazione dei dati.

Dubbi su questi tipi di software: il loro utilizzo, innanzitutto, non è stato finora regolato a livello normativo.

Si tratta, poi, di sistemi che in una certa misura si autoalimentano 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 della 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”.

Infine, non si deve trascurare il fatto che la maggior parte di questi software sono coperti da brevetti depositati da aziende private, sicché non si può disporre di una piena comprensione dei meccanismi del loro funzionamento, con pregiudizio delle esigenze di trasparenza e di verifica indipendente della qualità e dell’affidabilità dei risultati da essi prodotti.

¹⁶ C. MORABITO, *La chiave del crimine*, in *Polizia Moderna*, luglio 2015, 36.

5.b) Social Network Analysis¹⁷. - Fin dalla loro comparsa come *medium* di interazione di massa nei primi anni Duemila, i *social media* sono rapidamente diventati una preziosa fonte di informazioni per ricercatori di tutti i campi.

Il primo e fondamentale elemento riguarda la moderna concezione delle identità reali e virtuali, non da concepirsi come separate ed indipendenti ma, al contrario, come estremamente interdipendenti e capaci di influenzare relazioni, motivazioni e azioni individuali ugualmente nello spazio virtuale e in quello reale.

Ancora si stenta a integrare nell'analisi delle informazioni provenienti dai *social media* e, in generale, dalle altre fonti di raccolta dati, le scienze sociali e più precisamente i processi umani. Tali processi si fondano sempre più su sistemi di relazione che si attuano anche nel *web*, e sono ormai un elemento insostituibile per sviluppare un'efficace comprensione e **prevenzione** delle nuove minacce, costantemente in evoluzione.

Più le nostre vite si collegano alla rete, più le nostre identità reali e virtuali si fondono, più informazioni rilevanti vengono condivise e sono rintracciabili per elaborare analisi che siano le più complete possibili.

La *Social media Intelligence*, o **Socmint**, è la più recente componente del ciclo di *Intelligence* che si concentra sulla raccolta e sull'analisi delle informazioni che vengono

¹⁷ Cfr. M. LOMBARDI, A. BURATO, M. MAIOLINO, *Dalla SOCMINT alla Digital HumInt. Ricomprendere l'uso dei Social nel ciclo di Intelligence*, in *Sicurezza, Terrorismo e Società*, 2/2015, 95; A. BURATO, *Social media Intelligence: un nuovo spazio per la raccolta di informazioni rilevanti*, in *Sicurezza, Terrorismo e Società*, 2/2015, 109; S. BARTOLUCCI, *Il ruolo dei social media nell'investigazione*, in *Sicurezza e Giustizia*, I/MMXVI, 37; S. BOSCHIN, *Soluzioni innovative applicate all'analisi investigativa rivolta allo studio delle reti criminali*, in *Sicurezza e Giustizia*, II/MMXVI, 41.

prodotte e scambiate attraverso i *social media*¹⁸. Alcuni **problemi** da porre: su quale piattaforma sta avendo luogo la conversazione? Qual è la natura dell'interazione? Qual è l'oggetto della ricerca? Domande che, attraverso le loro risposte, definiscono la natura strumentale della disciplina che non può prescindere da una visione più ampia, che coniughi il processo di analisi delle informazioni con una contestualizzazione sociologica attraverso un processo sintetico definito **Digital Humint**, connubio fruttuoso tra la pratica della *Humint (Human Intelligence)* e l'approccio legato alle nuove fonti *social*.

Nel mondo virtuale la rappresentazione di sé avviene in due momenti distinti: all'atto dell'apertura di un profilo (rappresentazione statica) e attraverso la costruzione progressiva dei contenuti che popolano il profilo stesso (rappresentazione dinamica). Lo studio delle due rappresentazioni, specie nelle loro discrepanze, è in grado di fornire elementi interessanti per l'elaborazione di un'analisi che tenga conto anche degli aspetti **sociologici** e non meramente dei dati aggregati circa le impostazioni dell'*account* o delle rilevazioni delle preferenze dell'utente. Altro strumento altamente significativo per la rappresentazione di sé è l'uso del linguaggio: come per il mondo reale, la condivisione anche *online* di un codice comunicativo è significativa dell'appartenenza a un determinato gruppo.

Aspetti come le modalità di creazione delle comunità *online*, il loro sistema di relazioni e la loro tipologia possono essere diversi rispetto a quelli che definiscono comunità o gruppi tradizionali. È altresì necessario precisare che esistono *social* pensati appositamente per ricreare una specie di copia della comunità reale (Facebook) e altri che invece creano gruppi che non hanno nessuna, se non minima, trasposizione effettiva nel mondo reale.

¹⁸ La Socmint è genericamente diretta a colmare una condizione di ignoranza e a favorire il processo decisionale. Attraverso la raccolta e l'analisi di dati originati da condotte che gli individui tengono in una dimensione virtuale quale è quella di Internet e dei *social media*, la Socmint si pone l'obiettivo di permettere al suo fruitore di comprendere i fatti e i fenomeni che si generano e svolgono in tale dimensione, di prevederne gli sviluppi e, in una qualche misura, di capire cosa avviene o avverrà nel mondo reale. I *social media* possono contenere dati e notizie rilevanti ai fini della tutela della sicurezza nazionale, della pubblica sicurezza e dell'ordine pubblico. Da qui l'interesse crescente da parte dei servizi di *Intelligence* a raccogliere e analizzare tali dati con l'obiettivo di identificare possibili minacce di natura terroristica (M.E. BONFANTI, *Social media Intelligence a salvaguardia dell'interesse nazionale. Limiti e opportunità di una pratica da sviluppare*, in U. Gori, L. Martino (a cura di), *Intelligence e interesse nazionale*, Aracne, 2015, 239). In argomento v. pure B. PELLERO, *Tutela del segreto delle comunicazioni e sorveglianza elettronica nell'era dei social network e dell'Internet delle cose*, in *Gnosis - Riv. It. Intelligence*, 2/2016, 129.

Dal punto di vista del processo di *Intelligence*, in riferimento all'analisi dei profili individuali risulta assai interessante il tema della dimostrazione di amicizia e/o fedeltà.

In definitiva, v'è la possibilità di migliorare la sicurezza pubblica: se infatti lo spazio *online* viene sempre più frequentemente utilizzato per organizzare e coordinare attività criminali, i *social media* possono fornire uno strumento di inestimabile valore nella loro individuazione.

La raccolta del materiale condiviso attraverso i *social media* deve avere solide basi metodologiche: data l'enorme quantità di informazioni a disposizione, la selezione del campione di quelle da analizzare riveste invero un ruolo fondamentale. Purtroppo questo processo spesso risulta più focalizzato sulla raccolta di ampi campioni, tralasciando la rappresentatività degli stessi. Nelle scienze sociali il valore del campione prescelto è ritenuto di gran lunga più significativo del mero numero di dati raccolti, che potrebbero non contenere informazioni rilevanti ai fini dell'analisi.

Con particolare riferimento alle sole risorse testuali, una delle tecniche impiegate per l'analisi è l'estrazione automatica del loro significato: tale operazione consente di isolare il materiale rilevante dividendolo in categorie utili alla corroborazione e all'impiego delle informazioni.

Tuttavia, il raggiungimento di tale obiettivo è reso complesso, fra l'altro, dalla valutazione del contesto e dal concetto di gruppo nello spazio *online*. La rilevazione del contesto nel quale lo scambio di informazioni avviene passa attraverso la capacità di delineare la situazione e la cultura che lo hanno prodotto. D'altra parte, alcuni gruppi *online* condividono una sorta di identità linguistica (abbreviazioni, modi di dire, espressioni comuni) che li rendono facilmente identificabili: a tal proposito, la sociologia digitale fornisce basi teoriche per la comprensione delle sub-culture che si sviluppano sui *social media* e dei diversi utilizzi del linguaggio che li caratterizzano.

Infine, si deve tener conto di aspetti quali l'*observation effect* e il *gaming*. Il primo si configura come la tendenza a cambiare il proprio comportamento qualora si sia consapevoli di essere osservati, mentre il secondo riguarda il rilascio intenzionale di informazioni errate o volutamente ambigue: una volta appurata la presenza di tali fenomeni, l'informazione filtrata e

isolata si arricchisce di livelli di confidenza che possono essere supportati da ulteriori verifiche tramite la triangolazione con altre fonti.

5.c) Investigazioni difensive preventive. - L'attività investigativa preventiva è contemplata dall'art. 391 *nonies* c.p.p., ai sensi del quale l'attività investigativa del difensore, con esclusione degli atti che richiedono l'autorizzazione o l'intervento dell'autorità giudiziaria, può essere svolta anche dal difensore che ha ricevuto apposito mandato per l'**eventualità** che si instauri un procedimento penale.

Il mandato è rilasciato con sottoscrizione autenticata e contiene la nomina del difensore e l'indicazione dei fatti ai quali si riferisce.

In sostanza, le parti private potenziali (che potrebbero diventare indagato od offeso) possono incaricare il difensore anche **prima** che la notizia di reato sia iscritta nel registro: ad una persona può derivare un pregiudizio irrimediabile per il solo fatto che sia presentata una denuncia o che un altro imputato abbia fatto una chiamata in correità. Da ciò deriva la necessità che il difensore dell'interessato proceda ad indagini per sostenere la propria versione dei fatti. Analogo potere spetta alla persona offesa¹⁹.

Si tratta in altri termini di un'attività pre-procedimentale, in quanto finalizzata a ricercare ed individuare elementi di prova a favore del proprio assistito, ma destinati ad essere utilizzati soltanto nell'eventualità che si instauri un procedimento penale.

L'attività investigativa preventiva può essere svolta nelle seguenti ipotesi:

- nessuna iscrizione è stata effettuata in relazione al fatto al quale si riferisce l'investigazione;
- è stata iscritta una notizia di reato soggettivamente non qualificata;
- l'attività di indagine è compiuta su mandato di una persona diversa da quella il cui nominativo sia stato iscritto nel registro *ex art. 335 c.p.p.*;
- l'attività investigativa è compiuta dalla persona offesa dal reato al fine di provocare l'avvio di un procedimento o la riapertura di un procedimento penale già archiviato o

¹⁹ P. TONINI, *Manuale di procedura penale*, Giuffrè, 2018, 663.

l'emissione di un provvedimento di revoca della sentenza di non luogo a procedere o per fare emergere siffatta qualità nell'ambito di un procedimento pendente;

- in vista di una richiesta di revisione.

È necessaria, affinché si attivi un'investigazione preventiva, quantomeno l'**intuizione** di un pericolo di instaurazione di un procedimento penale a proprio carico, intravedendosi nella **pronosticabile** assunzione della qualità di persona sottoposta alle indagini la premessa per il compimento di atti altrimenti difficilmente organizzabili sul piano finalistico ed esposti al rischio di produrre risultanze irrilevanti²⁰.

La norma, esigendo una mera indicazione dei fatti, allude ad un'attività enunciativa dalla portata meno pregnante rispetto a quella tipica della descrizione; ma l'indicazione del fatto di riferimento non può essere talmente generica da vanificare la funzione delimitativa che la norma le assegna, perché sulla coincidenza di essa con la descrizione contenuta nell'eventuale atto del PM si giocherà la partita dell'**utilizzabilità** procedimentale degli atti d'indagine preventivamente compiuti.

Resta fermo che il difensore e gli altri soggetti di cui all'art. 391 *bis* c.p.p. non hanno obbligo di denuncia neppure relativamente ai reati dei quali abbiano avuto notizia nel corso delle attività investigative, anche preventive, da essi svolte (art. 334 *bis* c.p.p.): ovvio che non siano obbligati a denunciare la persona nel cui interesse investigano; ma non lo sono nemmeno su reati altrui, scoperti in quel lavoro²¹.

D'altro canto, è legittima ed utilizzabile l'attività svolta da un investigatore privato, prima dell'iscrizione della notizia di reato, al di fuori dell'ambito applicativo dell'art. 391 *nonies* c.p.p., atteso che l'attivazione dello statuto codicistico previsto per l'attività investigativa preventiva è rimessa alla volontà del soggetto, avendo natura del tutto facoltativa²².

²⁰ L. SURACI, *Le indagini difensive*, Giappichelli, 2014, 274.

²¹ F. CORDERO, *Procedura penale*, Giuffrè, 2006, 904.

²² Cass. pen., Sez. IV, n. 13110/2019.

6. Spunti per un metodo investigativo difensivo. - Con la Legge n. 397/2000 sulle indagini difensive è nata di fatto la figura dell'**avvocato-investigatore**, che ha facoltà di svolgere investigazioni per ricercare ed individuare elementi di prova a favore del proprio assistito; egli concretizza il diritto – dell'imputato e della persona offesa – di difendersi: prima conoscendo, poi decidendo consapevolmente e infine, eventualmente, provando.

Per risultare efficaci, le investigazioni dovrebbero procedere con un **metodo** che coinvolga sia l'uomo (competenza + intuito) che l'IA.

Di seguito un elenco di **problemi** che l'avvocato-investigatore si deve porre di fronte a un caso:

- vi è già un procedimento penale o vi è l'eventualità che esso si instauri? Ha senso promuovere un giudizio di revisione?
- è opportuno incaricare un investigatore privato autorizzato per indagini atipiche?
- sono necessarie specifiche competenze? È opportuno incaricare un consulente tecnico/criminologo?
- potrebbe servire un consulente tecnico matematico, statistico o informatico?
- è opportuno acquisire notizie attraverso colloqui non documentati?
- è opportuno chiedere una dichiarazione scritta?
- è opportuno chiedere di rendere informazioni da documentare²³?
- se si stanno assumendo informazioni da persone minori, ci si deve avvalere dell'ausilio di un esperto in psicologia o in psichiatria infantile?
- è opportuno richiedere della documentazione alla Pubblica Amministrazione?
- è opportuno accedere a luoghi pubblici, a luoghi privati o non aperti al pubblico?
- è necessario accertare le tracce e gli altri effetti materiali del reato con un accesso ai luoghi di abitazione e loro pertinenze?
- è opportuno presentare al PM o al giudice gli elementi di prova a favore del proprio assistito?

²³ Sul reato di false dichiarazioni al difensore, v. S. DI PINTO, *Il reato di false dichiarazioni al difensore*, in www.associazionelaic.it.

Orbene, l'IA può essere d'aiuto all'avvocato-investigatore nel rispondere a tali quesiti: l'idea è di associare in modo automatizzato una serie di osservazioni ad una serie di possibili risultati.

Lo scopo è una Difesa "informata": un'attività di ricerca, di raccolta, di valutazione, di elaborazione e di analisi di notizie per trasformarle in informazioni e costruire così basi di conoscenza per decisioni processuali.

Nel campo della giustizia predittiva, infine, i *tools* possono essere impiegati come ausilio per il difensore nell'adozione delle strategie processuali: ad esempio, conoscere l'orientamento della giurisprudenza di un certo tribunale sull'applicazione di una norma o sul trattamento sanzionatorio mediamente applicato per determinati reati potrebbe orientare verso la scelta di riti alternativi.