Università degli Studi della Campania *Luigi Vanvitelli*

MATERIALI E STUDI DI DIRITTO PUBBLICO

COLLANA DIRETTA DA

GIULIANO BALBI - LORENZO CHIEFFI

GIULIANO BALBI - FEDERICA DE SIMONE
ANDREANA ESPOSITO - STEFANO MANACORDA
(*a cura di*)

DIRITTO PENALE E INTELLIGENZA ARTIFICIALE

"NUOVI SCENARI"

IUSTITIAM COLIMUS

G. Giappichelli Editore – Torino

Università
degli Studi
della Campania
Luigi Vanvitelli

MATERIALI E STUDI DI DIRITTO PUBBLICO

COLLANA DIRETTA DA
GIULIANO BALBI - LORENZO CHIEFFI

NUOVA SERIE

18

Giuliano Balbi - Federica De Simone
Andreana Esposito - Stefano Manacorda
(*a cura di*)

DIRITTO PENALE E INTELLIGENZA ARTIFICIALE

"NUOVI SCENARI"

G. Giappichelli Editore – Torino

VIA PO 21 - TEL.: 011-81.53.111 - FAX: 011-81.25.100

http://www.giappichelli.it

ISBN/EAN 978-88-921-2461-5
ISBN/EAN 978-88-921-7771-0 (ebook - pdf)

Il presente volume viene pubblicato nella Collana Materiali e Studi di diritto pubblico previa positiva valutazione da parte della direzione scientifica condotta attraverso il sistema della *peer review*.

The use of AI neural networks in the fight against corporate crimes – AI.CO.CRI. 5.0

Nel Volume sono confluiti i risultati del progetto di ricerca svolto nell'ambito del Programma VALERE 2020: VAnviteLli per la RicERca, dell'Università degli Studi della Campania Luigi Vanvitelli.

Stampa: Stampatre s.r.l. - Torino

Indice

pag.

pag.

pag.

pag.

Prefazione

MARIAVALERIA DEL TUFO

Questo volume, agile e interessante, è curato da Giuliano Balbi, Andreana Esposito, Stefano Manacorda e da Federica De Simone, che da qualche anno esplora con competenza e passione le interferenze tra nuove tecnologie e diritto penale. Il lavoro è il risultato di un progetto scientifico portato avanti da un gruppo di ricercatori dell'Università degli Studi della Campania "Luigi Vanvitelli" in rapporto al tema peculiare dei *corporate crimes*, arricchito da contributi di prestigiosi studiosi esterni che hanno partecipato al più ampio e vivace dibattito instauratosi all'interno dell'Ateneo su tale *focus* di ricerca, analizzato anche in una prospettiva più ampia.

La promozione di attività di studio e di confronto è infatti principalmente finalizzata a riflettere sugli scenari che le nuove tecnologie aprono alla scienza, alla politica e al diritto. Continuamente rafforzato da scoperte e nuove modalità applicative, l'attuale strumentario scientifico e tecnologico pone problemi di gestione e controllo, generando nel contempo accettazione e diffidenza.

Soprattutto nei mesi della pandemia, l'applicazione generalizzata, anche all'interno di istituzioni pubbliche, di mezzi informatici ha reso definitivamente evidenti e acquisiti i vantaggi che l'uso virtuoso della tecnologia può apportare alla funzionalità di un sistema; ha familiarizzato milioni di persone con i nuovi strumenti rendendoli utilizzabili su larga scala e ha aperto strade da cui non appare opportuno tornare indietro, apparendo opzione più saggia – e irrinunciabile – l'integrazione di modalità, procedimenti ed esperienze.

Tuttavia è difficile pensare che l'utilizzo delle nuove tecnologie, una volta rese accessibili, disponibili, meglio conoscibili e più fruibili da un elevato numero di consociati, possa essere limitato o messo a frutto soltanto in una prospettiva orientata a perseguire e osservare regole già consolidate. Lo strumento in sé è neutro ma suscettibile di impieghi insidiosi, e dovrebbe essere rimessa alla responsabilità, alla affidabilità e alla sensibilità democratica di coloro che ne fanno uso la capacità di valutare potenzialità e rischi della sua utilizzazione stabilendone di volta in volta limiti e condizioni di fruizione. Un uso sapiente dovrebbe comunque permettere di modificare le regole senza soverchi timori e senza scardinare i principi, in modo da usufruire delle opportunità limitando la portata del

pericolo di applicazioni improprie. O si tratta di un cammino senza ritorno, destinato a non essere illuminato dai principi, ma capace di travalicarli al servizio di altri assetti sociali basati sul controllo?

Va infatti riconosciuto che le prestazioni offerte sono di tale rilievo da aver già iniziato a produrre mutamenti profondi che investono non solo il mondo esterno ma anche il nostro approccio ad esso, determinando il nascere di nuove sensibilità e nuove visioni. Il che non è necessariamente un male, ma soltanto un passaggio con antecedenti storici similari, riscontrabili in occorrenza di mutate condizioni di contesto.

Venendo a quel che più direttamente ci compete, le innovazioni tecnologiche, già apportate con successo in alcuni settori e allo studio in altri, stanno dando vita anche a timori e inquietudini. Tuttavia, mi chiedo come un ragazzino di oggi, che può ottenere moltissime cose con un click, tendenzialmente inserito in un modello culturale improntato all'*hic et nunc*, possa un domani tollerare i tempi lunghi della giustizia o piuttosto preferire che vengano utilizzate diverse modalità di intervento legate alla tecnologia, in grado di fornire soluzioni più performanti e immediate, anche accettando margini di errore o di rischio. E se soluzioni di questo tipo siano effettivamente perturbanti.

In altri termini, dobbiamo prendere in conto che, nell'immediato, le nuove tecnologie possono sicuramente offrire vantaggi evidenti anche se rilette, utilizzate e gestite nell'ottica di una società già stabilizzata intorno a regole generali condivise – e penso ad esempio ai controlli da parte delle forze dell'ordine di luoghi pericolosi con mezzi elettronici, a vicende endo-processuali tecnologicamente risolvibili, al supporto offerto dall'intelligenza artificiale a giudici e avvocati. Tuttavia, a medio/lungo termine, laddove la scienza avrà raggiunto risultati più avanzati e il progressivo utilizzo dei nuovi mezzi avrà modificato nel profondo rapporti, mentalità, sensibilità e modi di percepire, il discorso si porrà in modo diverso, perché sarà proprio l'*acquis* culturale a essere cambiato e a determinare le esigenze, i risultati attesi e le soglie di accettazione. E allora vanno poste oggi le basi perché tutto ciò possa essere affrontato con consapevolezza e rigore, nel pieno rispetto dei principi irrinunciabili e della dignità umana.

I rischi non mancano, anche a livello macro. Possibilità prima precluse – e sicuramente molto inquietanti – si dischiudono agli Stati: penso ad esempio all'acquisizione di dati sulla popolazione che possono diventare strumenti efficienti in termini di controllo sociale o per l'implementazione di politiche attive anche di emarginazione, esclusione o negazione di diritti fondamentali. Uno scenario già in parte attuato, con cui è urgente confrontarsi.

Una *mise en alerte* sull'uso delle nuove tecnologie è dunque importante per

bilanciare con visione razionale e serena i vantaggi che esse indubbiamente apportano e per rendere avvertiti i consociati dei rischi derivanti proprio dai mutamenti ormai fortemente radicati nel nostro contesto sociale e nel nostro vissuto. Un osservatorio implementato sul nucleo di principi non negoziabili che connota un diritto penale democratico appare allora quanto mai necessario: e questo libro, problematico e acuto, costituisce un contributo importante alla riflessione.

Introduzione

FEDERICA DE SIMONE

Il progresso tecnologico che sta caratterizzando la storia recente dell'umanità si contraddistingue per la velocità con cui si impone e, stando alla celebre espressione dell'economista Rosenberg, costituisce ancora una *scatola nera* di cui non si conoscono compiutamente i legami con l'innovazione. Ciò determina, da un lato, un senso di disorientamento rispetto alle conseguenze che ne possono derivare, dall'altro, la difficoltà di immaginare gli scenari futuri e predisporre gli strumenti per affrontarli.

Il giurista è naturalmente portato a risolvere le innovazioni classificando e regolamentando; tuttavia, si avverte anche nel mondo del diritto l'inadeguatezza degli strumenti ordinari e l'inopportunità di una visione ristretta alle categorie tradizionali. Cionondimeno, diffusa è la consapevolezza delle potenzialità e dei benefici che l'implementazione delle nuove tecnologie può apportare alla collettività, ma altrettanto diffusa è la consapevolezza della necessità di garantire la tutela dei diritti fondamentali.

Il volume contiene le riflessioni di alcune autorevoli voci in dottrina e di giovani ricercatori che hanno preso parte al Progetto di Ricerca *AI.CO.CRI 5.0: The use of AI neural networks in the fight against corporate crimes* finanziato dall'Università degli Studi della Campania Luigi Vanvitelli nell'ambito del Programma *Valere 2020*. Con questa raccolta di scritti si intende indagare i rapporti tra il Diritto penale e le nuove tecnologie, anche fornendo possibili chiavi di lettura in riferimento ad alcuni temi specifici.

In particolare, dopo aver esaminato i possibili impieghi e i diversi ruoli che l'intelligenza artificiale può rivestire nell'ambito delle attività di polizia, nella decisione giudiziaria e nella valutazione della pericolosità criminale, si affronta il tema della responsabilità penale classica nell'ipotesi in cui il reato non sia commesso direttamente dall'uomo, bensì dalla macchina.

La prospettazione di una responsabilità diretta dell'intelligenza artificiale a fronte della sua capacità decisionale, piuttosto che di una responsabilità collettiva da ravvisare in capo a coloro che hanno provveduto a crearla, programmarla e gestirla, porta al tema dei rapporti tra i nuovi sistemi e la *compliance* aziendale. Il binomio responsabilità societaria e nuove tecnologie è una questione tra le

più interessanti da indagare, non soltanto in quanto entrambe fortemente caratterizzate dal paradigma della predizione, ma anche per i possibili impieghi nelle politiche di contrasto alla corruzione. Il sistema *Zero Trust* progettato in Cina promette di essere un efficace strumento nel contrasto nella maggior parte delle ipotesi di reati contro la pubblica amministrazione. Tuttavia, gli effetti distorsivi che ne possono derivare hanno determinato i suoi stessi ideatori a sospenderne l'utilizzo.

Entrambi gli argomenti costituiscono l'oggetto principale su cui si sono sviluppate le due direttrici di indagine del progetto di ricerca e che hanno portato ad alcune valutazioni di opportunità circa le possibilità che l'impiego delle nuove tecnologie contribuisca a migliorare l'efficienza della spesa pubblica, aumentare la trasparenza e combattere proprio la corruzione.

Rimanendo in tema di responsabilità delle persone giuridiche, si è approfondita la questione dei rischi connessi all'impiego delle criptovalute rispetto alla fattispecie di riciclaggio, nella misura in cui le monete virtuali possono rappresentare uno strumento di *money laundering* utilizzato nell'interesse e a vantaggio delle società. Nel volume è riportata l'opinione contraria di chi ritiene che tale tecnologia possa costituire, invece, un modello di comportamento idoneo proprio a prevenire i fenomeni di riciclaggio, non ostando a ciò l'anonimato garantito dal mezzo informatico.

Suggestiva la prospettazione di un sistema capace di smascherare le menzogne e garantire, così, l'affermazione della verità, tra le massime ambizioni della società contemporanea. È quanto propone di fare il sistema di *memory detection* denominato a-IAT e sperimentato nel processo penale e sulla cui validità e ammissibilità nel novero delle prove scientifiche si è operata una riflessione, a seguito delle pronunce della giurisprudenza di merito sul tema.

Altra questione trattata è quella relativa al rapporto tra i benefici per la sicurezza della collettività e i rischi che ne possono derivare per la tenuta del sistema dei diritti fondamentali in tema di utilizzo massivo degli strumenti di riconoscimento facciale. Il dibattito sull'opportunità di un simile uso è molto fervido – sia in Europa, sia in Italia – e solleva non poche perplessità sull'opportunità dell'affermazione di una società del controllo, dubbi atti a incidere anche sulle scelte del legislatore.

Le finalità di predizione, prevenzione e scoperta del crimine sono sottese agli strumenti di intelligenza artificiale sempre più diffusi tra le forze dell'ordine di tutto il mondo e in dotazione anche al corpo dei Carabinieri per le tradizionali attività di indagine; l'impiego dei nuovi strumenti si sta rivelando un fondamentale ausilio, sia per le attività relative al controllo del territorio, sia per quelle strettamente connesse al contesto investigativo.

Altrettanto interessante si è rivelato il tema dell'utilizzo delle nuove tecnologie, in particolare della *blockchain*, nel contrasto al fenomeno delle frodi ali-

mentari, ambito per il quale la normativa penalistica ha sempre mostrato tutti i suoi limiti in termini di efficacia. Proprio la sinergia con gli strumenti di recente acquisizione costituisce lo spunto per una riflessione sull'opportunità di una rivisitazione e sistematizzazione dell'intera materia, in modo da garantire la salute collettiva dai possibili rischi derivanti da condotte penalmente rilevanti in tema di sicurezza alimentare.

Prima ancora di fornire una chiave di lettura rispetto ai singoli temi imposti dalla rivoluzione tecnologica, i contributi racchiusi in questo volume costituiscono sono essi stessi lo specchio del dibattito in atto. Ad oggi, infatti, sembrano contrapporsi due schieramenti, chi predilige un approccio di *esaltazione progressista* della tecnologia e, diversamente, chi assume una posizione di sfiducia tecnologica. Eppure, una visuale laica sulla questione è possibile. È necessario contemperare una riflessione epistemologica del rapporto tra la tecnica e l'uomo con una visione antropocentrica, che ponga l'uomo al centro dei processi di innovazione, permettendo di superare la cd. reificazione della tecnologia, che riduce il pensiero computazionale a un processo di *datificazione*.

«*Dobbiamo lavorare per umanizzare la tecnologia ed evitare che la tecnologia ci disumanizzi*», e se lo dice il robot *Sophia*…

CAPITOLO I

Intelligenza artificiale e diritto penale: qualche aggiornamento e qualche nuova riflessione

FABIO BASILE

SOMMARIO: 1.1. Premessa. – 1.2. Che cosa intendiamo per intelligenza artificiale? – 1.3. Primo ambito – IA e attività di *law enforcement*. – 1.3.1. RoboCop: dalla fantascienza alla realtà? – 1.3.2. Sistemi di intelligenza artificiale e polizia predittiva. – 1.4. Secondo ambito – IA e decisione giudiziaria: la macchina-giudice? – 1.5. Terzo ambito – IA e valutazione della pericolosità criminale: gli algoritmi predittivi. – 1.6. Quarto ambito – IA e responsabilità penale: così intelligente da essere "responsabile"? – 1.6.1. IA strumento del reato. – 1.6.2. IA autore del reato? – 1.6.2.1. Irriducibilmente umano?

1.1. *Premessa*

Nel presente contributo ho scelto di riprendere sinteticamente alcune tematiche già trattate in un precedente scritto uscito nel 2019 [1], integrandole con alcuni aggiornamenti e alcune nuove riflessioni maturate grazie – oltre che a nuove letture – anche al confronto con colleghi e giovani studiosi che ho potuto avere in occasione di numerosi seminari e convegni sull'IA, tenutisi negli ultimi 24 mesi.

Nelle pagine seguenti cercherò, pertanto, di re-indagare i possibili ambiti all'interno dei quali la rivoluzione tecnologica messa in moto dall'IA già solleva, o è destinata a sollevare, problemi, dubbi e questioni, rilevanti per il diritto penale:

1. le attività di *law enforcement*, in particolare le attività di cd. *polizia predittiva*;
2. i cd. *automated decision systems*, che potrebbero in futuro conoscere un

[1] F. BASILE, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Dir. pen. uomo*, 2019, p. 1 ss. Ringrazio il dott. Alessandro Carlini per i preziosi suggerimenti e per la revisione del testo che qui si offre ai lettori.

impiego anche all'interno dei procedimenti penali, sostituendo, in tutto o in parte, la decisione del giudice-uomo;

3. i cd. *algoritmi predittivi*, impiegati per valutare la pericolosità criminale di un soggetto, vale a dire la probabilità che costui commetta in futuro un (nuovo) reato;

4. infine, le possibili ipotesi di coinvolgimento – come strumento, come autore, o come vittima – di un sistema di IA nella commissione di un reato.

Il punto di partenza è, ovviamente, il medesimo dal quale partivo due anni fa: l'intelligenza artificiale è ovunque [2]. Le sue applicazioni pratiche si trovano nelle abitazioni, nelle automobili, negli uffici, nelle banche, negli ospedali, nel cielo e in internet, incluso l'"internet delle cose". Le animazioni di Hollywood, i videogiochi, i navigatori satellitari, il motore di ricerca di Google, sono tutti basati su tecniche di intelligenza artificiale. E così a proseguire [3].

È quindi facile presagire che la rivoluzione tecnologica messa in moto dall'intelligenza artificiale potrà presto significativamente impattare anche con le pretese di tutela dei beni giuridici affidate al diritto penale [4].

E noi, come giuristi, come penalisti, non possiamo farci trovare impreparati, «giacché quello che è veramente inquietante» – scriveva Martin Heidegger – «non è che il mondo si trasformi in un completo dominio della tecnica. Di gran lunga più inquietante è che l'uomo non è affatto preparato a questo radicale mutamento del mondo» [5].

Pare, pertanto, opportuno continuare a condurre la riflessione, già avviata, sulle possibili implicazioni dell'IA sul sistema della giustizia penale, al fine di non aggravare il ritardo del diritto, in particolare del diritto penale italiano, di fronte all'evoluzione tecnologica.

In effetti, come è stato efficacemente rilevato, «il progresso irrompe, non chiede permesso. E nel contesto attuale disegnare questo nuovo rapporto tra esseri umani e macchine non è per niente facile. Anche perché le tecnologie digitali hanno una velocità impressionante. Le tecnologie di ieri, come ad esempio la

[2] M.A. BODEN, *L'intelligenza artificiale*, Il Mulino, Bologna, 2019, p. 3.

[3] Per una sistematica ricognizione sugli usi attuali dell'IA e nel futuro prossimo prevedibile, vedi P. STONE, R. BROOKS, E. BRYNJOLFSSON, R. CALO, O. ETZIONI, G. HAGER, J. HIRSCHBERG, S. KALYANAKRISHNAN, E. KAMAR, S. KRAUS, K. LEYTON-BROWN, D. PARKES, W. PRESS, A. SAXENIAN, J. SHAH, M. TAMBE, A. TELLER, *Artificial Intelligence and Life in 2030. One Hundred Year Study on Artificial Intelligence: Report of the 2015-2016 Study Panel*, Stanford, 2016, p. 18 ss.

[4] In tema di rapporti tra IA e giustizia penale v. V. MANES, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in *DisCrimen*, 15 maggio 2020.

[5] M. HEIDEGGER, *Gelassenheit*, 1959, trad. it. di A. Fabris, *L'abbandono*, Il Melangolo, Genova, 1995, p. 36.

TV, la radio, l'elettricità, l'automobile hanno impiegato più di 50 anni per raggiungere i 50 milioni di utenti. Ci hanno concesso tutto il tempo per abituarci alle loro innovazioni, per avere nuove regole sul loro utilizzo, e per organizzare le nostre vite e le nostre società di conseguenza. Oggi, le tecnologie digitali irrompono molto più velocemente, e non ci danno affatto il tempo per organizzarci e per abituarci alle loro dirompenti innovazioni. Un esempio evidente di questa velocità viene dalle reti sociali: Twitter ha impiegato meno di 3 anni per raggiungere i 50 milioni di utenti; Facebook e Instagram meno di 2 anni. Anche se il record della velocità è quello di Pokemon Go, che è riuscito a raggiungere i 50 milioni di download in soli 19 giorni!» [6].

1.2. *Che cosa intendiamo per intelligenza artificiale?*

Prima, però, di entrare nel merito delle tematiche "penalistiche", conviene richiamare l'attenzione su alcune caratteristiche dei sistemi di IA, rilevanti ai fini della nostra indagine.

1. Innanzitutto, quando parliamo di IA non dobbiamo necessariamente pensare ad un "umanoide" simile in tutto e per tutto all'essere umano: l'umanoide può essere, sì, un'applicazione di IA (forse la più eclatante), ma di certo non l'unica e non, almeno nella fase attuale, la più rilevante dal punto di vista pratico [7]. Per contro, possiamo affermare che oggi l'IA è, principalmente, un *software*, una componente algoritmica.

2. In secondo luogo, per quanto possa essere suggestivo parlare di intelligenza artificiale, occorre rimarcare che l'intelligenza (quella degli esseri umani, prima ancora che quella delle macchine), benché oggetto di numerosissimi studi di psicologi, biologi e neuroscienziati, costituisce ancora un concetto indeterminato [8]. Ad ogni modo, l'intelligenza artificiale è mimesi, è copiatura delle presta-

[6] G.F. ITALIANO, *Intelligenza artificiale, che errore lasciarla agli informatici*, in *Agendadigitale.eu*, 11 giugno 2019, p. 3.

[7] Così C. TREVISI, *La regolamentazione in materia di Intelligenza artificiale, robot, automazione: a che punto siamo*, in *Medialaws*, 21 maggio 2018, p. 1; L. FLORIDI, *What the Near Future of Artificial Intelligence Could Be*, in *Philosophy & Technology*, 32, 2019, p. 11 ss.

[8] Si noti, per altro verso, che proprio dagli studi sull'intelligenza artificiale stanno pervenendo importanti contributi per scoprire come funziona l'intelligenza umana e il cervello umano. Si veda, ad esempio, un recente progetto europeo di integrale simulazione del cervello umano, realizzato grazie all'impiego di tecniche di IA: Redazione (a cura di), *Il progetto europeo sul cervello umano*, in *Dir. pen. uomo*, 2 aprile 2019. Dall'altra parte dell'Atlantico, un progetto USA analogo è in svolgimento: Redazione (a cura di), *L'esortazione del Presidente*, ivi, 2 aprile 2019.

zioni umane: i sistemi di IA "apprendono" per correlazioni [9], e non seguono il ragionamento deduttivo-causale, tipico dell'intelligenza umana.

3. Oggi si riconosce unanimemente che i grandi e rapidi progressi, compiuti dall'IA in tempi recenti, sono stati consentiti dalla felice combinazione di due fattori [10]:

– da un lato, il recente, impressionante aumento delle capacità computazionali, grazie alle quali disponiamo di computer sempre più veloci, potenti, con capacità di memoria (e, quindi, tra l'altro, di archiviazione dati) straordinariamente grandi;

– dall'altro lato, il recente, impressionante aumento di dati digitali, raccolti anche grazie a sensori ad alta definizione e a basso costo: dati alla cui raccolta contribuiamo ogni giorno anche noi digitalizzando documenti, scattando foto, facendo video o inviando messaggi tramite le reti sociali o altri strumenti di messaggistica.

4. La combinazione di tali due fattori – unitamente ad altri progressi nella ricerca – ha, tra l'altro, consentito di elaborare e di diffondere su larga scala i sistemi di *machine learning* che possiamo, in estrema sintesi, descrivere così: il sistema di IA "impara" autonomamente dall'ambiente esterno (tramite i dati che immagazzina ed elabora), e modifica le proprie prestazioni adattandole agli esiti del procedimento di apprendimento [11]. In altri termini, il *software* di IA programma sé stesso nel tempo in modo funzionale all'obiettivo assegnato.

[9] Questo è particolarmente vero per i sistemi di IA che fanno uso del cd. *machine learning*. Tuttavia, esiste almeno un altro grande approccio all'IA, la cd. IA Simbolica, la quale tenta di riprodurre il ragionamento umano.

[10] Così, tra i tanti, J. KAPLAN, *Intelligenza artificiale. Guida al futuro prossimo*, Luiss University Press, Roma, II ed., 2018, p. 72; G.F. ITALIANO, *Intelligenza artificiale: passato, presente, futuro*, in F. Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, Torino, 2018, p. 220; R. CALO, *Artificial Intelligence Policy: a Primer and Roadmap*, in *University of Bologna Law Review*, 3, 2, 2018, p. 186.

[11] Sul *machine learning*, v., in una prospettiva tecnica, S. RUSSELL, P. NORVIG, *Artificial Intelligence: A Modern Approach,* Chennai, III ed., 2009, p. 634 ss.; L. FLORIDI, *What the Near Future of Artificial Intelligence Could Be*, cit., p. 4 ss.; P. DOMINGOS, *L'algoritmo definitivo: la macchina che impara da sola e il futuro del nostro mondo*, Bollati Boringhieri, Torino, 2016, p. 7 ss.; K. HAO, *What is machine learning*, in *MIT Technology Review*, 17 novembre 2018; C. COLAPIETRO, A. MORETTI, *L'intelligenza Artificiale nel dettato costituzionale: opportunità, incertezze e tutela dei dati personali*, in *BioLaw Journal*, 3, 2020, p. 365 ss.; F. SUMAN, *Dove sta andando oggi l'Intelligenza artificiale?*, in *Il Bo Live*, 11 marzo 2019; in una prospettiva giuridica, R. CALO, *Artificial Intelligence Policy*, cit., p. 185; H. SURDEN, *Machine Learning and Law*, in *Washington Law Review*, 89, 1, 2014, p. 87 ss.; S. QUINTARELLI, *Forum AI and Law*, in *BioLaw Journal*, 1, 2020, p. 493 ss.

1.3. *Primo ambito – IA e attività di* law enforcement

1.3.1. *RoboCop: dalla fantascienza alla realtà?*

Probabilmente molti di noi ricordano la figura di RoboCop, il poliziotto con un corpo di titanio e kevlar, un cervello informatico e sensori ultrapotenti: se nel 1987, anno di uscita del celebre film, tale immagine apparteneva decisamente alla fantascienza («il futuro della legge» era il sottotitolo del film), oggi la realtà ci propone alcune applicazioni delle tecnologie di IA – in uso, per lo più in via sperimentale, presso le forze di polizia di alcuni Stati – che si avvicinano molto a RoboCop [12]: si tratta, nella maggior parte dei casi, di macchine robotiche, non necessariamente umanoidi, utilizzate per una varietà di compiti, come ad esempio attività di pattugliamento, sorveglianza, disinnesco di bombe, individuazione di atteggiamenti sospetti, riconoscimento facciale, etc. [13].

Applicazioni di questo tipo, se da un lato hanno il gran merito di preservare da una serie di pericoli gli agenti (umani), e se in talune circostanze assicurano un ottimo livello di efficienza nelle prestazioni erogate, sollevano, dall'altro lato, una serie di problematiche:

– la questione della *privacy*, in considerazione della gran mole di dati che queste applicazioni (fornite, ad esempio, di sensori e telecamere avanzate) possono acquisire in relazione alla vita, anche privata, dei cittadini: dati che, peraltro, potrebbero essere manipolati abusivamente, sottratti, deformati, con grave pregiudizio per le persone cui essi si riferiscono;

– alcune di queste applicazioni sono equipaggiate con armi, non letali (ad esempio, il *taser* o lo *spray* al peperoncino) o letali (equiparabili alle classiche

[12] In argomento, v. N. SHARKEY, *2084: Big robot is watching you. Report on the future of robots for policing, surveillance and security*, 2008, reperibile al seguente indirizzo *web https://it.scribd.com/document/139971746/Noel-Sharkey-2084-Big-robot-is-watching-you-Future-Robot-Policing-Report-Final*; una versione più breve di tale saggio, intitolata *The robot arm of the law grows longer*, e originariamente pubblicata sulla rivista *Computer*, 2009, p. 113, può essere letta anche a questo indirizzo *web https://ieeexplore.ieee.org/document/5197441*; v. pure L. ROYAKKERS, R. VAN EST, *A Literature Review on New Robotics: Automation from Love to War*, in *International Journal of Social Robotics*, 7, 5, 2015, p. 549 ss.; E.E. JOH, *Policing Police Robots*, in *UCLA Law Review Discourse*, 2016, p. 516; L. PASCULLI, *Genetics, Robotics and Crime Prevention*, in D. PROVOLO, S. RIONDATO, F. YENISEY (a cura di), *Genetics, Robotics, Law, Punishment*, Padova University Press, Padova, 2014, p. 197 ss.; per una disamina più generale sull'uso della IA nelle attività di *law enoforcement*, v. P. STONE *et al.*, *Artificial Intelligence and Life in 2030*, cit., p. 36 ss.

[13] Un sofisticato programma di riconoscimento facciale – SARI, Sistema Automatico di Riconoscimento Immagini – è in dotazione anche alla Polizia scientifica italiana, stando a quanto si apprende dalle notizie giornalistiche, v. redazione ANSA, *Ladri individuati grazie al nuovo sistema di riconoscimento facciale*, 7 settembre 2018.

armi da fuoco), il che crea indubbie preoccupazioni in ordine al tasso di fallibilità di queste applicazioni e quindi in ordine all'individuazione del responsabile (uomo o macchina?) di eventuali uccisioni o lesioni commesse per errore, nonché in ordine alla presumibile assenza, in capo a questi dispositivi robotizzati armati, di doti tipicamente umane – la pietà, l'intuito, la capacità di improvvisazione, il cd. senso comune [14] – la cui presenza, in operatori della polizia, è sempre auspicabile [15];

– vi è, poi, il problema dell'ampiezza che il controllo umano deve assumere su tali applicazioni: il controllo dell'uomo si deve limitare alla scelta degli obiettivi, al monitoraggio, o deve essere un controllo più intenso, esercitato anche a costo di compromettere le prestazioni stesse del RoboCop?

Suona inquietante, se riguardato in questa prospettiva, il fatto che il *sequel* del film RoboCop, uscito nel 2014, avesse come sottotitolo: «chi avrà il controllo: l'uomo o il robot?» [16].

1.3.2. *Sistemi di intelligenza artificiale e polizia predittiva*

Oltre ai RoboCop, in relazione alle attività di *law enforcement* dobbiamo anche citare le possibili applicazioni dei sistemi di IA per finalità di polizia predittiva, laddove 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 cui quelli relativi a notizie di reati precedentemente commessi, agli spostamenti e alle attività di soggetti sospettati, ai luoghi, teatro di ricorrenti azioni criminali, e alle caratteristiche di questi luoghi, al periodo del-

[14] Come giustamente sottolinea M.B. MAGRO, *Biorobotica, robotica e diritto penale*, in D. PROVOLO, S. RIONDATO, F. YENISEY (a cura di), *Genetics, Robotics, Law, Punishment*, cit., p. 512, «ai robot dotati di intelligenza artificiale, dotati di conoscenze altamente specialistiche, manca, al di sotto di queste conoscenze, il livello di conoscenze comuni, il c.d. "senso comune", ciò che tutti gli umani posseggono senza aver fatto studi particolari. Il "senso comune" è quello che consente di collegare conoscenze specialistiche di campi diversi e di affrontare i problemi e di risolverli senza la rigidità tipica dell'approccio simbolico dell'intelligenza. Spesso una reazione intelligente ad una certa situazione è quella che, sì, tiene in considerazione il contesto, ma che non è capace di selezionare quale aspetto del contesto sia rilevante».

[15] Sulle cd. *autonomous weapons*, v. in particolare N. SHARKEY, *La robotica*, in J. AL-KHALILI (a cura di), *Il futuro che verrà*, Bollati Boringhieri, Torino, 2018, p. 195 ss.; R. CALO, *Artificial Intelligence Policy*, cit., p. 196, con ulteriori riferimenti.

[16] *https://www.youtube.com/watch?v=0BIWKVH8_GE*.

l'anno o alle condizioni atmosferiche maggiormente connesse alla commissione di determinati reati; tra i dati utilizzati a questi fini talora compaiono anche informazioni relative all'origine etnica, al livello di scolarizzazione, alle condizioni economiche, alle caratteristiche somatiche (… una rivincita di Lombroso?), riconducibili a soggetti appartenenti a determinate categorie criminologiche (ad es., potenziali terroristi), etc. [17].

In tempi recenti, l'impiego di *software* basati sull'IA ha consentito di fare un salto di qualità nelle attività di polizia predittiva, dal momento che è ora possibile l'acquisizione e la rielaborazione di una mole enorme di dati, che fa emergere connessioni prima difficilmente individuabili dall'operatore umano [18].

I *software* di polizia predittiva possono dividersi fondamentalmente in due categorie:

– quelli che, ispirandosi alle acquisizioni della criminologia ambientale, individuano le cd. "zone calde" (*hotspots*), vale a dire i luoghi che costituiscono il possibile scenario dell'eventuale futura commissione di determinati reati (ad es., il sistema informatico *X-LAW*, originariamente predisposto dalla Questura di Napoli, che parrebbe aver già ottenuto ottimi risultati sul territorio italiano nel campo della prevenzione di talune tipologie di reati [19]);

– quelli che, ispirandosi invece all'idea del *crime linking*, seguono le serialità criminali di determinati soggetti (individuati o ancora da individuare), per prevedere dove, come e quando costoro commetteranno il prossimo reato, identifi-

[17] Per un completo inquadramento della materia della *predictive policing*, v. W.L. PERRY, B. MCINNIS, C.C. PRICE, S.C. SMITH, J.S. HOLLYWOOD, *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*, Rand, Santa Monica, 2013.

[18] C. CATH, S. WACHTER, B. MITTELSTADT, M. TADDEO, L. FLORIDI, *Artificial Intelligence and the "Good Society": the US, EU, and UK approach*, in *Science and Engineering Ethics*, 2018, p. 505 ss.; L. BENNET MOSES, J. CHAN, *Algorithmic Prediction in Policing: Assumptions, Evaluation, and Accountability*, in *Policing and Society*, 2016, p. 1 ss.; G. MASTROBUONI, *Crime is Terribly Revealing: Information Technology and Police Productivity*, in *Review of Economic Studies*, 87, 6, novembre 2020, p. 2727 ss., consultabile *online* al seguente link: *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2989914*; per un sintetico quadro, in lingua italiana, dei sistemi di IA finalizzati ad attività di polizia predittiva, v. R. PELLICCIA, *Polizia predittiva: il futuro della prevenzione criminale?*, in *cyberlaws.it*, 9 maggio 2019; B. PEREGO, *Predictive policing: trasparenza degli algoritmi, impatto sulla privacy e risvolti discriminatori*, in *BioLaw Journal*, 2, 2020, p. 447 ss.; pur riferendosi a sistemi non solo di polizia predittiva v. C. MORELLI, *Furti e rapine: a sventarli ci pensa l'intelligenza artificiale!*, in *Altalex.com*, 6 maggio 2019.

[19] Notizie riferite da M. IASELLI, *X-LAW: la polizia predittiva è realtà*, in *Altalex.com*, 28 novembre 2018. Un sistema recentissimo di questo tipo, sempre di pregiata fattura italiana, è Pelta Suite, in sperimentazione nel Comune di Caorle. L. BARIELLA, *Polizia predittiva: al via la sperimentazione a Caorle*, in *Altalex.com*, 24 maggio 2021.

cando "la mano criminale", il *modus operandi* emergente dalla serie criminale (un esempio in tal senso è l'ormai noto *software* Delia della società KeyCrime).

Questi sistemi di polizia predittiva possono indubbiamente apportare grandi benefici, ma il loro utilizzo suscita più d'una perplessità [20]:

– essi possono fornire adeguate previsioni solo in relazione a limitate, determinate categorie di reati (ad esempio, reati attinenti alla criminalità da strada, come rapine e spaccio di stupefacenti), non necessariamente quelli più pericolosi per la democrazia e per la libertà democratica;

– il loro uso potrebbe implicare gravi attriti con la tutela della *privacy* (in considerazione della gran mole di dati personali raccolti), e con il divieto di discriminazione (nella misura in cui, ad esempio, identifichino fattori di pericolosità connessi a determinate caratteristiche etniche, o religiose o sociali) [21];

– 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, dando origine al fenomeno della "profezia che si auto-avvera": se, ad esempio, un *software* predittivo individua una determinata "zona calda", i controlli e i pattugliamenti 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", mentre altre zone, originariamente non ricondotte nelle "zone calde", e quindi non presidiate dalla polizia, rischiano di rimanere, o di diventare, per anni zone "fredde", ove la commissione di reati non viene adeguatamente monitorata;

– inoltre, questi sistemi sollecitano una prevenzione dei reati attraverso l'intervento attivo della polizia, attraverso, quindi, una sorta di "militarizzazione" nella sorveglianza di determinate zone o di determinati soggetti, senza invece minima-

[20] Le considerazioni contenute nel prosieguo del testo rielaborano spunti e riflessioni formulati da L. PASCULLI, *Genetics, Robotics and Crime Prevention*, cit., p. 192, e da R. PELLICCIA, *Polizia predittiva*, cit., che rinvia, tra l'altro, alle ricerche compiute in materia, e alle relative perplessità espresse, dall'Human Rights Data Analysis Group (HRDAG), raccolte nel sito *https://hrdag.org/usa/*, alla voce *The Problem with Predictive Policing*. Sulle stesse problematiche, più di recente v. anche B. PEREGO, *Predictive policing*, cit., p. 452 ss.

[21] Su questi aspetti, v. A. BONFANTI, *Big data e polizia predittiva: riflessioni in tema di protezione del diritto alla privacy e dei dati personali*, in *MediaLaws*, 24 ottobre 2018; E. THOMAS, *Why Oakland Police Turned Down Predictive Policing*, in *vice.com*, 28 dicembre 2016; J. KREMER, *The end of freedom in public places? Privacy problems arising from surveillance of the European public space*, Helsinki, 2017, in particolare il capitolo 3.4.2, "*Prediction*", p. 269 ss.; in particolare, sul ruolo dei dati nella discriminazione algoritmica prodotta dai sistemi di polizia predittiva, v. R. RICHARDSON, J. SCHULTZ, K. CRAWFORD, *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, in *New York University Law Review*, 94, 2019, p. 192 ss.

mente mirare alla riduzione del crimine attraverso un'azione rivolta, a monte, ai fattori criminogeni (fattori sociali, ambientali, individuali, economici, etc.);

– infine, non si deve trascurare il fatto che la maggior parte di questi *software* sono coperti da brevetti depositati da aziende private, le quali, a buon diritto, sono gelose 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. D'altra parte, se anche i meccanismi di funzionamento fossero resi pubblici, la logica di molti di essi potrebbe risultare comunque intrinsecamente non intelligibile nemmeno per un esperto di IA, dal momento che questi meccanismi si "autoalimentano" in modo imperscrutabile tramite il *machine learning* (cd. *black box*).

1.4. *Secondo ambito – IA e decisione giudiziaria: la macchina-giudice?*

Algoritmi basati sull'IA vengono, già da qualche tempo, utilizzati anche a fini decisionali nei più svariati ambiti [22]: si tratta dei cd. *automated decision systems*, in via di crescente diffusione [23], sia in ambito privato, sia in ambito pubblico [24].

Tra le decisioni che siffatti algoritmi sono in grado di assumere vi sono, ovviamente, anche decisioni finalizzate a comporre, o prevenire, liti e risolvere controversie.

Anzi, in quest'ambito, le nuove tecnologie – grazie alla possibilità di attingere a quantità enormi di dati da fonti quali banche-dati giurisprudenziali, legislative, raccolte di precedenti, e simili – hanno già messo a punto dispositivi molto sofisticati, che utilizzano teoria dei giochi, analisi dei risultati positivi e strategie di negoziazione per risolvere le questioni [25].

Anche queste applicazioni presentano indubbiamente taluni vantaggi, tra i quali:

[22] J. KLEINBERG, H. LAKKARAJU, J. LESKOVEC, J. LUDWIG, S. MULLIANATHAN, *Human Decisions and Machine Predictions*, in *Quarterly Journal of Economics*, 2017, p. 237.

[23] D. REISMAN, J. SCHULTZ, K. CRAWFORD, M. WHITTAKER, *Algorithmic Impact Assessments: a Practical Framework for Public Agency Accountability*, 2018, reperibile al seguente link: *https://ainowinstitute.org/aiareport2018.pdf*.

[24] Sull'impiego, all'interno della pubblica amministrazione, di sistemi decisionali basati sull'IA in Italia e in Argentina, v. ad esempio D.U. GALETTA, J.G. CORVALÀN, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in *federalismi.it*, 6 febbraio 2019, p. 1 ss.

[25] Per un primo inquadramento del possibile impatto delle tecnologie di IA sul processo penale, mi permetto di rinviare al seguente link: *https://www.youtube.com/watch?v=Tl8an9paY8M*.

– impiegano una metodologia che i soggetti coinvolti percepiscono come oggettiva e priva di pregiudizi [26];

– comportano una riduzione dei tempi e significativi risparmi di spesa sia per i soggetti coinvolti, sia per i soggetti responsabili della decisione [27].

Esse, tuttavia, suscitano inevitabilmente talune preoccupazioni, soprattutto se si pensa ad un loro possibile impiego anche in sede penale [28]:

– potrebbero essere fonte di discriminazioni e automatismi;

– mettono in crisi la tradizionale idea di "giudice naturale precostituito per legge" (art. 25, comma 1, Cost.), idea che finora aveva anche una proiezione geografica: il giudice-macchina sarà un giudice unico per tutto il territorio nazionale?

– anche il principio espresso dall'art. 101, comma 1, Cost. ne risulta scosso: può una macchina agire "in nome del popolo"?

– e che dire della "soggezione soltanto alla legge", richiesta dall'art. 101, comma 2, Cost.? il giudice macchina sarà, probabilmente, molto più vincolato al precedente, di quanto lo sia oggi il giudice uomo (perlomeno nei sistemi di *civil law*), con il rischio, peraltro, di ostacolare interpretazioni evolutive;

– infine, sembra pressoché impossibile aspettarsi da un algoritmo la capacità di intendere e applicare la regola di giudizio, di cui all'art. 533, comma 1, c.p.p., basata sull'"oltre ogni ragionevole dubbio", dal momento che possiamo immaginare *software* capaci di dare risposte secondo una logica binaria (sì/no; bianco/nero; vero/falso), o anche secondo una logica probabilistica (sì al 70%; bianco all'80%; vero al 90%), ma difficilmente *software* capaci di esprimere valutazioni, nella cui assunzione giochino un ruolo irrinunciabile – per quanto non ponderabile in termini precisi – fattori irriducibilmente umani [29].

[26] J. KAPLAN, *Intelligenza Artificiale*, cit., p. 137 ss.

[27] E. LATIFAH, A.H. BAJREKTAREVIC, M.N. IMANULLAH, *Digital Justice in Online Dispute Resolution: The Shifting from Traditional to the New Generation of Dispute Resolution*, in *Brawijaya Law Journal – Journal of Legal Studies*, 6, 1, aprile 2019.

[28] Tra gli altri, v. G. CANZIO, *Il dubbio e la legge*, in *Dir. pen. cont.*, 2018, p. 1 ss.; M. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assessment tools tra Stati Uniti ed Europa*, ivi, 29 maggio 2019, p. 1 ss.; A. NATALE, *Introduzione. Una giustizia (im)prevedibile?*, in *Quest. giust.*, 4, 2018, p. 1 ss.; nello stesso fascicolo, v. pure i contributi di C. COSTANZI, *La matematica del processo: oltre le colonne d'Ercole della giustizia penale*, e di C. CASTELLI, D. PIANA, *Giustizia predittiva. La qualità della giustizia in due tempi*; vedasi, infine, il fascicolo 7/2019 di *Giur. it.* che ospita un'ampia sezione monografica, a cura di U. Ruffolo ed E. Gabrielli, dedicata al tema *Intelligenza artificiale e diritto*.

[29] Sul punto, v. pure S. GABORIAU, *Libertà e umanità del giudice: due valori fondamentali della giustizia. La giustizia digitale può garantire nel tempo la fedeltà a questi valori?*, in *Quest. giust.*, 4, 2018, p. 11.

1.5. *Terzo ambito – IA e valutazione della pericolosità criminale: gli algoritmi predittivi*

Quali probabilità sussistono che un individuo, avente determinate caratteristiche, possa in futuro commettere un (nuovo) reato?

Si tratta di un quesito la cui risposta è necessaria, tra l'altro, quando si tratta di applicare una misura di sicurezza, una misura cautelare o una misura di prevenzione, o anche per concedere la sospensione condizionale di una pena o l'affidamento in prova al servizio sociale [30].

Ebbene, a tale fondamentale quesito oggi i nostri giudici forniscono risposte per lo più intuitive, affidate esclusivamente alla loro esperienza personale e al loro buon senso, oppure, quando consentito dalla legge, basate su valutazioni cliniche di periti [31], mentre in futuro (e già nel presente di altri ordinamenti giuridici) siffatte valutazioni prognostiche della pericolosità criminale potrebbero essere affidate a specifici algoritmi (*risk assessment tools*, o algoritmi predittivi), capaci di effettuare valutazioni attuariali, rielaborando quantità enormi di dati al fine di far emergere relazioni, coincidenze, correlazioni, che consentano di profilare una persona e prevederne i successivi comportamenti, anche di rilevanza penale [32].

Negli Stati Uniti, in effetti, già da una decina d'anni sono in fase di diffusione algoritmi predittivi della pericolosità criminale.

Essi sono, ad esempio, usati nella fase del *parole* (per decidere se un individuo, nelle more della celebrazione del processo, possa essere rilasciato dietro il pagamento di una eventuale cauzione), o per misurare il rischio di recidiva del condannato, ai fini della sua ammissibilità al *probation* o ad altra misura alternativa alla detenzione, o infine in sede di *sentencing.*

[30] Sui plurimi ambiti, all'interno dei quali risulta necessario formulare una prognosi di futura commissione di un (nuovo) reato, sia consentito rinviare a F. BASILE, *Esiste una nozione ontologicamente unitaria di pericolosità sociale? Spunti di riflessione, con particolare riguardo alle misure di sicurezza e alle misure di prevenzione*, in *Riv. it. dir. proc. pen.*, 2018, p. 644 ss.

[31] Sul cui grado di affidabilità, tuttavia, la dottrina è fortemente scettica: v., per tutti, J. MONAHAN, *Predicting violent behavior: An assessment of clinical techniques*, Sage Pubns, London, 1981.

[32] L. CASTELLETTI, G. RIVELLINI, E. STRATICÒ, *Efficacia predittiva degli strumenti di Violence Risk Assessment e possibili ambiti applicativi nella psichiatria forense e generale italiana*, in *Journal of Psychopathology*, 2014, p. 153 ss.; G. ROCCA, C. CANDELLI, I. ROSSETTO, F. CARABELLESE, *La valutazione psichiatrico forense della pericolosità sociale del sofferente psichico autore di reato: nuove prospettive tra indagine clinica e sistemi attuariali*, in *Riv. it. med. leg. dir. san.*, 4, 2012, p. 1442 ss.

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

Tuttavia, ancora una volta non possiamo rilevare anche alcune perplessità, espresse ad esempio in relazione al caso Loomis – in cui, in sede di *sentencing*, aveva trovato applicazione il *software* COMPAS – *Correctional Offender Management Profiling for Alternative Sanctions* – dalla Corte Suprema del Wisconsin:

– trattasi di un *software* coperto da segreto industriale, che impedisce la divulgazione di informazioni relative al suo metodo di funzionamento;

– esso effettua valutazioni su base collettiva, di gruppo, e non individuale;

– esso comporta il rischio di una sovrastima del rischio di commissione di reati a carico di talune minoranze etniche [33].

Ma soprattutto, come ormai gli stessi esperti di IA avvertono, occorre considerare (e ciò vale anche per gli altri due ambiti sopra esaminati) che l'algoritmo – qualsivoglia algoritmo – non è "neutro" [34]: nel concepire l'architettura di un algoritmo, il programmatore fa delle scelte che, necessariamente, influenzano il "risultato" dell'operazione computazionale.

1.6. *Quarto ambito – IA e responsabilità penale: così intelligente da essere "responsabile"?*

Droni che uccidono per le strade urbane [35] o su fronti lontani, impegnati nella lotta al terrorismo, auto senza conducente coinvolte nella causazione di inciden-

[33] Su questi aspetti, v. in particolare K. FREEMAN, *Algorithmic Injustice: How the Wisconsin Supreme Court Failed to Protect Due Process Rights in State v. Loomis*, in *North Carolina Journal of Law & Technology*, 18, 2016, p. 76.

[34] V. di recente le riflessioni del filosofo e psicoanalista M. BENASAYAG, *La tirannia dell'algoritmo*, Vita e Pensiero, Milano, 2020.

[35] N. SHARKEY, *La robotica*, cit., p. 197 riferisce, ad esempio, di un sospetto cecchino ucciso a Dallas tramite l'intervento di un drone (luglio 2016), commentando con le seguenti parole tale episodio: «in quel caso esisteva una chiara giustificazione e gli esperti di diritto hanno asserito che l'azione era stata legittima, resta il fatto che in quella circostanza si è probabilmente varcato un confine. È giusto proteggere la polizia, e la polizia dovrebbe, fintanto che è possibile, utilizzare mezzi non violenti. Quando questi si dimostrino inefficaci, è certamente necessario elevare il livello della forza impiegata, ma in modo graduale e proporzionale al reato che viene commesso: e sono valutazioni decisamente impegnative per un robot che agisce senza il controllo umano».

ti anche a danno di persone (come nel tragico investimento di una ciclista avvenuto nel marzo 2018 in Arizona [36]), *software* che eseguono, in collaborazione o addirittura in sostituzione dell'uomo, compiti sempre più sofisticati, come pilotare un grosso aereo, ma che qualche volta possono interferire negativamente con la condotta umana (come i recenti disastri aerei del Boeing 737 MAX hanno purtroppo dimostrato [37]): chi risponde dei fatti di reato in tal modo eventualmente commessi [38]? il programmatore del *software*? il suo produttore? il suo utilizzatore? o direttamente il sistema di intelligenza artificiale?

1.6.1. *IA strumento del reato*

Lo scenario relativamente più semplice è ovviamente quello in cui il sistema di intelligenza artificiale costituisce lo strumento – in mano a un uomo – attraverso il quale il reato viene commesso [39]. Le enormi potenzialità dell'intelligenza artificiale, infatti, potrebbero – e già lo sono state – essere asservite anche a scopi criminali e quindi essere utilizzate per la commissione di reati attraverso modalità fino a qualche anno fa assolutamente inimmaginabili: solo per fare due esempi, pensiamo a droni e sottomarini senza equipaggio, controllati a distanza, utilizzati per il trasporto di stupefacenti e armi illegali; oppure ai *social BOT*, che possono essere utilizzati come strumenti per realizzare molestie, diffamazioni, abusi della credulità popolare, attraverso *tweet*, *retweet* e altre diavolerie simili.

Dobbiamo, insomma, prepararci a un'era in cui la commissione di reati con lo strumento dell'intelligenza artificiale potrebbe diventare assai frequente e incisiva, anche in considerazione dell'accresciuta vulnerabilità di alcuni aspetti della vita umana connessi ad impieghi dell'intelligenza artificiale, a partire dall'impressionante numero di dati sul comportamento e sullo stile di vita di ciascuno di noi – facilitato da una condizione umana perennemente *Onlife* – che possono

[36] L. BUTTI, *Le auto guideranno da sole, ma con quali responsabilità?*, in *Il Bo Live*, 9 novembre 2018; F. SUMAN, *Dilemmi morali per le auto a guida autonoma*, ivi, 7 novembre 2018. Sul funzionamento delle *self-driving cars* e dei loro problemi tecnici nonché giuridici, v. H. SURDEN, M.A.WILLIAMS, *Technological Opacity, Predictability, and Self-Driving Cars*, in *Cardozo Law Review*, 38, 2016, p. 121 ss.

[37] G.F. ITALIANO, *Intelligenza artificiale*, cit.

[38] Sui cambiamenti che il largo utilizzo dei sistemi di IA potrebbe produrre sul sistema della responsabilità giuridica v. altresì le riflessioni di M.B. MAGRO, *Decisione umana e decisione robotica. Un'ipotesi di responsabilità da procreazione robotica*, in *Legisl. pen.*, 10 maggio 2020.

[39] S. RIONDATO, *Robotica e diritto penale (robot, ibridi, chimere, "animali tecnologici")*, in D. PROVOLO, S. RIONDATO, F. YENISEY (a cura di), *Genetics, Robotics*, cit., p. 600 ss.

essere raccolti tramite i vari canali informatici, fino all'eventuale instaurazione di rapporti di vera dipendenza, talora anche affettiva, da macchine e sistemi di servizio che si muovono per noi, lavorano per noi, custodiscono i nostri anziani e i nostri figli.

L'uomo rischia, insomma, di ritrovarsi in balìa della macchina, sguarnito dei presidi tradizionali di protezione, essendo tali presidi concepiti e strutturati per proteggerlo da "attacchi umani".

Sorge allora un primo interrogativo: abbiamo bisogno di nuove fattispecie di reato? O abbiamo bisogno di rimodellare quelle già esistenti, al fine di renderle applicabili alla realizzazione di condotte criminose attraverso lo strumento dell'intelligenza artificiale, offrendo così tutela ai beni giuridici anche da questa nuova fonte di attacchi?

1.6.2. *IA autore del reato?*

Gli esempi sopra formulati, che finora abbiamo presentato come ipotesi in cui l'intelligenza artificiale è lo strumento in mano all'uomo, potrebbero, però, presentarsi anche in uno scenario in cui la mano dell'uomo scompare, o diventa pressoché impercettibile.

Nel caso, infatti, in cui nella realizzazione del reato sia coinvolto un sistema di intelligenza artificiale di ultima generazione, che risulti fornito di capacità di apprendimento e di autonomia decisionale, potremmo chiederci se non risulti già varcata la frontiera del futuro, tanto da potersi individuare direttamente nel sistema di intelligenza artificiale l'"autore" del reato.

Quando le scelte, le valutazioni, i bilanciamenti sottesi alla commissione di un fatto di reato non sono più opera esclusiva dell'uomo, ma sono quanto meno "condivisi con", se non interamente delegati alla macchina, ecco che il percorso di attribuzione delle responsabilità indubbiamente si complica.

Vengono in mente scenari in parte già noti.

Come si individua il responsabile di un'attività svolta in *équipe*? Come si individua il colpevole in quelle ipotesi in cui il procedimento decisionale ed esecutivo è parcellizzato, frazionato e distribuito in capo a una pluralità di soggetti?

La novità sta però ora nel fatto che tra i membri delle *équipe*, tra i plurimi soggetti coinvolti, non vi sono più solo esseri umani, ma anche sistemi di intelligenza artificiale, col conseguente innesco di un processo di "alienazione della responsabilità" dall'agente umano [40], giacché l'agente umano si colloca lontano – nel tempo, nello spazio e nel processo decisionale – rispetto all'offesa al bene giuridico.

C'è allora il rischio di creare zone franche, sacche di illiceità all'interno delle

[40] C. BAGNOLI, *Teoria della responsabilità*, Il Mulino, Bologna, 2019, p. 77.

quali non è possibile imputare alcuna responsabilità alla persona fisica. E, se del reato non risponde l'uomo, chi ne dovrà rispondere?

Ecco, quindi, che occorre porci un nuovo interrogativo: *machina delinquere potest?* [41]

A dire il vero, la questione della possibile attribuzione di responsabilità ad entità diverse dall'uomo non è una novità assoluta. Platone, nelle Leggi, attribuiva la responsabilità anche ad animali e cose [42]; ancora, alle soglie dell'illuminismo, venivano celebrati processi penali a carico di animali "delinquenti" [43] e, dal 2001, anche in Italia è stata configurata una responsabilità da reato in capo agli enti, a carico quindi di persone che sono tali solo per effetto di una *fictio* giuridica.

L'ultima frontiera è segnata dai sistemi di intelligenza artificiale.

Possono essi essere considerati persone? O, quanto meno, possono essere assimilati alle persone, al fine di un'attribuzione di responsabilità non solo civile, ma anche penale [44]?

[41] La suggestiva formula *machina delinquere non potest* (che noi qui riprendiamo sopprimendo il "non" ed aggiungendo il punto di domanda) – formula la quale a sua volta ricalca l'antico brocardo *societas delinquere non potest*, a lungo invocato per precludere una responsabilità da reato a carico degli enti – è stata coniata da A. CAPPELLINI, *Machina delinquere non potest. Brevi appunti su intelligenza artificiale e responsabilità penale*, in *Criminalia*, 2018, p. 499 ss.

[42] Come ci ricorda, da ultimo, C. BAGNOLI, *Teoria della responsabilità*, cit., p. 72.

[43] Riferimenti in A. CAPPELLINI, *Machina delinquere non potest*, cit., p. 20; C. BAGNOLI, *Teoria della responsabilità*, cit., p. 73.

[44] Il dibattito in materia è stato inizialmente avviato dai filosofi del diritto e dai filosofi dell'informatica (v., tra gli altri, H. JONAS, *The Imperative of Responsibility. In search of an Ethics for the Technological Age*, University of Chicago Press, Chicago, 1984; L.B. SOLUM, *Legal Personhood for Artificial Intelligences*, in *North Carolina Law Review*, 70, 1992, p. 1231, ora in *Illinois Public Law and Legal Theory Research Papers*, 9-13, 20 marzo 2008; L. FLORIDI, J.W. SANDERS, *On the Morality of Artificial Agents*, in *Minds and Machines*, 14/3, 2004, p. 349 ss.; B.C. STAHL, *Information, Ethics, and Computers: The Problem of Autonomous Moral Agents*, ivi, 14, 2004, p. 67 ss.; ID., *Responsible Computers? A Case for Ascribing Quasi-Responsibility to Computers Independent of Personhood or Agency*, in *Ethics and Information Technology*, 8, 2006, p. 205 ss.; G. SARTOR, *Gli agenti software: nuovi soggetti del ciberdiritto*, in *Contratto e impresa*, 2, 2002, p. 57 ss.), e si è di recente acceso anche tra gli studiosi della responsabilità civile (si veda, ad esempio, A. SANTOSUOSSO, C. BOSCARATO, F. COROLEO, *Robot e diritto: una prima ricognizione*, in *Nuova giur. civ. comm.*, II, 2012, p. 497 ss.; A. SANTOSUOSSO, *If the agent is not necessarily a human being. Some legal thoughts*, in D. PROVOLO, S. RIONDATO, F. YENISEY (a cura di), *Genetics, Robotics, Law, Punishment*, cit., p. 545 ss., nonché il volume U. RUFFOLO (a cura di), *Intelligenza artificiale e responsabilità*, Giuffrè, Milano, 2018) e tra i costituzionalisti (si veda, ad esempio, il volume a cura di F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, cit.).

La risposta positiva comporterebbe di pagare un prezzo molto alto: la disponibilità ad ammettere una colpevolezza "extra-umana".

Possiamo davvero parlare di un coinvolgimento soggettivo dell'autore-macchina al fatto commesso? Possiamo concepire una rimproverabilità, per l'appunto personale, della macchina? Possiamo parlare di capacità di intendere e di volere, in relazione a una rete neurale? Possiamo configurare una "colpa" o addirittura un "dolo" dell'algoritmo [45]?

C'è chi dice di sì [46], facendo leva sui recenti progressi fatti nella robotica, nella percezione e nel *machine learning*, supportati dai miglioramenti sempre più veloci della tecnologia informatica, al punto che oggi la frase di buonsenso comunemente accettata secondo la quale "i computer fanno solo quello che sono programmati a fare" non sarebbe più vera [47].

Accanto, peraltro, al quesito *machina delinquere potest*?, occorrerà subito dopo porsi anche il connesso quesito: (*quomodo*) *machina puniri potest*?, con quali pene? e perseguendo quale tra le possibili funzioni della pena?

1.6.2.1. *Irriducibilmente umano?*

Eppure, di fronte a questo possibile scenario, qualcosa ci lascia inquieti. La responsabilità penale è personale, cioè "della persona": davvero potremo assimilare, ai fini dell'allocazione della responsabilità penale, la macchina all'uomo? Oppure c'è qualcosa che la persona umana ha e che la macchina non potrà mai avere? [48]

[45] Su quest'ultimo interrogativo, v. D. FALCINELLI, *Il dolo in cerca di una direzione penale. Il contributo della scienza robotica ad una teoria delle decisioni umane*, in *Arch. pen.*, 1, 2018, p. 9.

[46] Tra gli scienziati di IA, fornisce una convinta risposta affermativa alle questioni formulate nel testo, J. KAPLAN, *Intelligenza artificiale*, cit., p. 153: «un sistema di IA può commettere reati? La risposta è sì»; ID., *Le persone non servono. Lavoro e ricchezza nell'epoca dell'intelligenza artificiale*, Luiss University Press, Roma, 2016, p. 80. Tra gli studiosi di diritto penale, la posizione più avanzata è quella sostenuta da Gabriel Hallevy, i cui lavori sono oggetto di una meditata presentazione critica da parte di A. CAPPELLINI, *Machina delinquere non potest*, cit., p. 10 ss., e di M. BASSINI, L. LIGUORI, O. POLLICINO, *Sistemi di Intelligenza Artificiale, responsabilità e accountability. Verso nuovi paradigmi?*, in F. PIZZETTI (a cura di), *Intelligenza artificiale*, cit., p. 363 ss., ai quali, pertanto, è in questa sede possibile rinviare.

[47] J. KAPLAN, *Intelligenza artificiale*, cit., p. 19.

[48] Vedi le stimolanti riflessioni in proposito di Massimo Cacciari, in M. CACCIARI, S. ARCIERI, F. BASILE, R. BIANCHETTI, P.E. CICERONE, *Alla radice dell'imputabilità e della colpevolezza penali. Conversazione con Massimo Cacciari – pt. 2*, in *Dir. pen. uomo*, 13 gennaio 2021. Inoltre, vedi le acute e ancora attuali riflessioni di E. AGAZZI, *Alcune osservazioni sul*

Forse un'"intelligenza" superiore? Ahi, questo purtroppo no: l'intelligenza dei computer sta ormai superando quella degli esseri umani [49], almeno a livello prestazionale.

Forse la "coscienza del dis-valore sociale" della propria condotta? o i "sentimenti", che le macchine non hanno e che probabilmente mai avranno? Probabilmente no, dal momento che coscienza del dis-valore sociale e sentimenti non sono elementi necessari per fondare una responsabilità penale.

Allora il "libero arbitrio"? Be', le neuroscienze hanno ampiamente messo in discussione il libero arbitrio dell'uomo [50].

Ma se escludiamo l'intelligenza, la coscienza, i sentimenti, il libero arbitrio, cosa rimane ancora di irriducibilmente umano?

Qual è lo *specificum* dell'uomo? Che cosa potrebbe impedire, come ultima Thule, una piena assimilabilità della macchina all'uomo, anche ai fini della responsabilità penale?

problema dell'intelligenza artificiale, in *Riv. fil. neo-scolastica*, 59, 1, 1967, p. 1 ss., il quale – da ottimo filosofo della scienza quale egli è – partendo dal presupposto che nulla è logicamente impossibile, mette in luce come l'uomo sia dotato di un misterioso e indefinibile *quid pluris*, che plasma tutte quelle attività squisitamente umane, noto come "intenzionalità", che ad oggi le macchine non hanno (ancora) replicato. Sulle medesime questioni vedi altresì J.R. SEARLE, *La mente è un programma?*, in *Le scienze*, 259, 1990, p. 16 ss.

[49] V. pure quanto affermato da S. Hawking durante la Conferenza *Zeitgeist*, Londra, maggio 2015: «nell'arco dei prossimi cento anni, l'intelligenza dei computer supererà quella degli esseri umani» [citazione riportata da Redazione (a cura di), *Do You Trust This Computer?*, in *Dir. pen. uomo*, 15 maggio 2019; v. la notizia anche su *Newsweek* (L. WALKER, *Stephen Hawking warns artificial intelligence could end humanity*, 14 maggio 2015)].

[50] In particolare v. J. KAPLAN, *Intelligenza artificiale*, cit., p. 113 ss., il quale mette in discussione la concezione tipicamente occidentale e cartesiana del libero arbitrio, attingendo alle ultime scoperte neuroscientifiche e a conoscenze matematico-informatiche di lunga data (in particolare ai cd. problemi indecidibili).

CAPITOLO II

Reati colposi e tecnologie dell'intelligenza artificiale

ALBERTO CAPPELLINI

SOMMARIO: 2.1. Introduzione. Autorìa "artificiale intelligente" e responsabilità colposa. – 2.2. Macchine intelligenti e imprevedibilità tecnologica. – 2.3. Il "*responsibility gap*" e le problematiche regolative dell'attribuzione di colpa: i riflessi sull'imputazione ai produttori umani. – 2.4. (*Segue*). I riflessi sull'imputazione agli utilizzatori umani. – 2.5. IA, colpa, caso fortuito: la politicità della soglia del rischio consentito e le influenze della precauzione. – 2.6. Riflessioni conclusive: quali prospettive per il futuro?

2.1. *Introduzione. Autorìa "artificiale intelligente" e responsabilità colposa*

Lo sviluppo impetuoso delle tecnologie dell'intelligenza artificiale, e la prospettiva di una penetrazione via via più diffusa di strumenti tecnologici "intelligenti" nelle società contemporanee, ha condotto la riflessione penalistica più recente a interrogarsi sui numerosi profili di intersezione che tali innovazioni hanno con il diritto penale. Uno dei campi forse più futuristici, ma certamente ricco di precipitati in un domani neanche poi così lontano, è quello di come la responsabilità penale più classica – quella individuale, dei soggetti umani – subisca modificazioni quando il reato non sia commesso immediatamente per mano dell'autore, bensì per mezzo di strumenti a carattere artificiale intelligente [1].

[1] Non sono pochi, ormai, i lavori generali sul tema, anche solo limitandosi alla lingua italiana. Per tutti: C. PIERGALLINI, *Intelligenza artificiale: da "mezzo" ad "autore" del reato?*, in *Riv. it. dir. proc. pen.*, 2020, p. 1743; I. SALVADORI, *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale*, in *Riv. it. dir. proc. pen.*, 2021, p. 83; A. GIANNINI, *Intelligenza artificiale,* human oversight *e responsabilità penale: prove d'impatto a livello europeo*, in *disCrimen*, 21 novembre 2022; B. MAGRO, *Robot, cyborg e intelligenze artificiali*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (diretto da), *Cybercrime*, Utet-Wki, Milano, 2019, p. 1179; EAD., *Biorobotica, robotica e diritto penale*, in D. PROVOLO, S. RIONDATO, F.

Come spesso accade, talvolta la realtà supera la fantasia nel proporre all'attenzione degli operatori una casistica concreta che già oggi è più variegata di quanto si immagini possibile [2].

YENISEY (eds), *Genetics, robotics, law, punishment*, Padova University Press, Padova, 2014, p. 499; S. RIONDATO, *Robotica e diritto penale (robots, ibridi, chimere e "animali tecnologici")*, ivi, p. 599; ID., *Robot: talune implicazioni di diritto penale*, in P. MORO, C. SARRA (a cura di), *Tecnodiritto. Temi e problemi di informatica e robotica giuridica*, Francoangeli, Milano, 2017, p. 85; U. PAGALLO, *Saggio sui robot e il diritto penale*, in S. VINCIGUERRA, F. DASSANO (a cura di), *Scritti in memoria di Giuliano Marini*, Esi, Napoli, 2010, p. 595; ID., *Robotica*, in U. PAGALLO, M. DURANTE (a cura di), *Manuale di informatica giuridica e diritto delle nuove tecnologie*, Utet, Torino, 2012, p. 141; R. BORSARI, *Intelligenza Artificiale e responsabilità penale: prime considerazioni*, in *MediaLaws*, 3/2019, p. 262; V. MANES, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in *disCrimen*, 15 maggio 2020, p. 2; U. RUFFOLO, *Machina delinquere potest? Responsabilità ed "illeciti" (anche penali?) della "persona elettronica" e tutele per gli agenti software autonomi*, in ID. (a cura di), *XXVI Lezioni di Diritto dell'Intelligenza Artificiale*, Giappichelli, Torino, 2021, p. 295; P. SEVERINO, *Intelligenza artificiale e diritto penale*, in U. RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè Francis Lefebvre, Milano, 2020, p. 533; EAD., *Le implicazioni dell'intelligenza artificiale nel campo del diritto con particolare riferimento al diritto penale*, in P. SEVERINO (a cura di), *Intelligenza artificiale, Politica, economia, diritto, tecnologia*, Luiss University Press, Roma, 2022; V. ARAGONA, *I Robot: the criminal liability of artificial intelligences*, in *TransJus Working Papers Publications*, 4/2019, p. 83. Per un inquadramento più ampio del tema entro quello più generale dei rapporti tra IA e giustizia penale, fondamentale F. BASILE, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Dir. pen. uomo*, 29 settembre 2019, oltre al successivo ID., *Intelligenza artificiale e diritto penale: qualche aggiornamento e qualche nuova riflessione*, in F. BASILE, M. CATERINI, S. ROMANO (a cura di), *Il sistema penale ai confini delle* hard sciences*. Percorsi epistemologici tra neuroscienze e intelligenza artificiale*, Pacini, Pisa, 2021, p. 11 (nel cennato volume, esattamente sul tema, va altresì ricordato il lavoro di G.R. MINELLI, *Quando l'autore del reato è un robot: tra vecchi modelli imputativi e nuovi possibili paradigmi di responsabilità penale*, p. 57, oltre a vari interessanti spunti negli altri contributi, fra cui E. LO MONTE, *Intelligenza artificiale e diritto penale: le categorie dommatiche alla prova del futuribile*, p. 41). Più incentrato sulla sola tematica in questione un ulteriore contributo di F. BASILE, *Diritto penale e Intelligenza Artificiale*, in *Giur. it.*, 2019, suppl., p. 67. Sia consentito, infine, un riferimento fin d'ora, una volta per tutte, al nostro A. CAPPELLINI, Machina delinquere non potest*? Brevi appunti su intelligenza artificiale e responsabilità penale*, in *Criminalia*, 2018, p. 499, per una ricostruzione dell'argomento dell'IA come agente del reato, e della possibilità di "punire" quest'ultimo. La letteratura straniera sul tema, invece, è troppo ampia per essere qui sistematicamente ricordata: si rinvia, per tutti, ai richiami di cui alle note che seguono, oltre che ai riferimenti bibliografici di cui già al nostro scritto da ultimo citato.

[2] Fra la casistica "bizzarra" già verificatasi, si può ricordare, solo a titolo di esempio, l'utilizzo di sottomarini robotici per traffici di droga: U. PAGALLO, *The Laws of Robots. Crimes, Contracts and Torts*, Springer, Dordrecht, 2013, p. 65. Per un panorama generale, attuale e possibile futuro, degli *AI crimes*: T.C. KING, N. AGGARWAL, M. TADDEO, L. FLORIDI, *Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions*,

Eppure, al di là delle pressoché infinite possibilità con cui i più diversi reati previsti dall'ordinamento possono combinarsi con modalità commissive che passano attraverso l'azione materiale di un soggetto artificiale intelligente, ve ne è una che merita particolare attenzione. Essa, infatti, forse più di tutte, è gravida di importanti conseguenze che già si possono avvertire e che si può probabilmente preconizzare non mancheranno di emergere per frequenza, importanza pratica e rilievo teorico in futuro.

Il riferimento è ai reati colposi contro la vita e l'incolumità individuale [3].

L'orizzonte verso cui si stanno muovendo le tecnologie in questione – come sempre accade nelle moderne società industriali-capitalistiche – è infatti quello che, al di là di iniziali prototipi unici o limitati nel numero, cerca di "confezionare" l'intelligenza artificiale in prodotti standardizzati da assemblare in serie, abbattendo così i costi di produzione, e poi immettere sul mercato. L'introduzione in massa di questi "prodotti artificiali intelligenti" nel tessuto sociale, non può che riproporre all'attenzione degli operatori – *mutatis mutandis* – quel problema fondamentale della sicurezza degli utenti e di terzi che solitamente ricade sotto l'etichetta dei profili di responsabilità per danno da prodotto [4], ma che in tale sce-

in *Science and Engineering Ethics*, 2020, p. 89; M. CALDWELL, J.T.A. ANDREWS, T. TANAY, L.D. GRIFFIN, *AI-enabled future crime*, in *Crime Science*, 2020.

[3] Fra i lavori specificamente dedicati al tema del rapporto tra autorìa artificiale e reati colposi, per tutti: S. BECK, *Intelligent agents and criminal law – Negligence, diffusion of liability and electronic personhood*, in *Robotics and Autonomous Systems*, 2016, p. 138; EAD., *Google Cars, Software Agents, Autonomous Weapons Systems – New Challanges for Criminal Law*, in E. HILGENDORF, U. SEIDEL (eds), *Robotics, Autonomics and the Law*, Nomos, Baden-Baden, 2017, p. 227; A. MORAITI, *AI Crimes and Misdemeanors: Debating the Boundaries of Criminal Liability and Imputation*, in G. VERMEULEN, N. PERŠAK, N. RECCHIA (eds), *Artificial Intelligence, Big Data and Automated Decision-Making in Criminal Justice*, Maklu, Antwerpen, 2021, p. 109 (nel medesimo volume va ricordato altresì B. PANATTONI, *AI and Criminal Law: The Myth of "Control" in a Data-Driven Society*, p. 125, dal taglio tematico invero un po' più ampio).

[4] Nella penalistica italiana, sulla responsabilità per danno da prodotto cfr., per tutti: C. PIERGALLINI *Danno da prodotto e responsabilità penale. Profili dommatici e politico-criminali*, Giuffrè, Milano, 2004; ID., *La responsabilità del produttore: una nuova frontiera del diritto penale?*, in *Dir. pen. proc.*, 2007, p. 1125 (studi dei quali il ricordato recente scritto ID., *Intelligenza artificiale: da "mezzo" ad "autore" del reato?*, cit., è espressamente presentato come una "continuazione"); D. CASTRONUOVO, *Responsabilità da prodotto e struttura del fatto colposo*, in *Riv. it. dir. proc. pen.*, 2005, p. 301; A. BERNARDI, *La responsabilità da prodotto nel sistema italiano: profili sanzionatori*, in *Riv. trim. dir. pen. econ.*, 2003, p. 1. Un nesso tra le due tematiche è sottolineato altresì da S. GLESS, E. SILVERMAN, T. WEIGEND, *If robots cause harm, who is to blame? Self-driving cars and criminal liability*, in *New Criminal Law Review*, 2016, p. 426. Sul tema del rapporto tra IA e danno da prodotto cfr. anche R. BERTOLESI, *Intelligenza artificiale e responsabilità penale per danno da prodotto*, Università degli Studi di Milano, Tesi dottorale, a.a. 2018/2019.

nario – a ben vedere – pare estendersi fino a coinvolgere ambiti di responsabilità per colpa più classici e tradizionali [5].

In effetti, la diffusione ampia di tali tipologie nuove di prodotti, anche con l'adozione dei massimi standard di sicurezza possibili, inevitabilmente provocherà un certo numero di sinistri, con danno per l'incolumità umana. Anzi, per la verità simili eventi si sono già verificati: anche solo limitandosi al settore applicativo delle tecnologie dell'IA forse più ampio, quello delle auto a guida autonoma, sono moltissimi gli accadimenti nefasti, anche mortali, di cui si ha ad oggi notizia [6].

Ma, a ben vedere, è la struttura stessa del reato colposo che fa sì che la rilevanza pratica di una prospettiva di rischio vada al di là della mera frequenza statistica – magari in realtà rara – degli incidenti. Certamente il delitto d'evento non può sussistere a prescindere da un accadimento di danno. Ma d'altro canto è vero anche che le regole cautelari, le quali stabiliscono i limiti dell'attività in questione, hanno l'obiettivo di prevenire – a monte – uno spettro di prospettive lesive quanto mai ampio e variegato. Insomma, anche quando il momento "patologico" – l'incidente-evento e, correlativamente, il reato colposo di risultato – sia statisticamente infrequente, è indubbio come l'idea di prevenzione e di tutela dai rischi che informa (in particolare ma non solo) le attività industriali complesse plasmi con prepotenza tutta la disciplina del fenomeno, anche nella sua fisiologia. Così, in breve, l'atteggiamento che l'ordinamento assume nei confronti della prospettiva-limite – l'incidente mortale, il disastro – si ripercuote a ritroso venendo a influenzare in ogni parte e aspetto le varie, singole attività che caratterizzano il vivere sociale. Fino a che punto consentirle, regolamentarle attraverso l'introduzione di cautele e come distribuire tra i vari "partecipanti" le responsabilità conseguenti, sono scelte che dipendono da delicate operazioni di bilanciamento tra interessi in gioco, valutazioni costi/benefici che dipendono in modo ampiamente significativo anche dalla prospettiva dell'eventualità ultima, più recondita e negativa [7].

[5] Quali – come si dirà meglio *infra* – la colpa stradale, la colpa medica, e così via.

[6] Due gli episodi più ricordati: Williston (Florida, USA), 7 maggio 2016, una vettura Tesla modello S si infilava sotto ad un camion bianco, non riuscendo a distinguerlo dal cielo luminoso, distruggendo completamente l'abitacolo e provocando così la morte del conducente; Tempe (Arizona, USA) 18 marzo 2018, una vettura Uber completamente autonoma investiva un pedone, provocandone la morte. Ma ne sono avvenuti altri anche altri. Alcuni mortali: Mountain View (California, USA) 23 marzo 2018; Houston (Texas, USA), 17 aprile 2021. Molti altri – difficili peraltro anche da tracciare in fonti ufficiali e non – con conseguenze meno gravi.

[7] Si tratta di valutazioni che definiscono la soglia di quello che è penalisticamente noto come *rischio consentito*. Nel contesto contemporaneo della *società del rischio* vi è sostanziale convergenza di opinioni circa la natura politico-valutativa di un simile giudizio, e dell'importante ruolo della *paura* (che sovente si presenta nella veste di *precauzione*) nella scelta

In tale quadro, è innegabile la carica sostanziale, di valore, della questione. Essa infatti incrocia, da un lato, l'entità e la portata della penetrazione delle tecnologie dell'IA nel tessuto sociale che si ritenga opportuno autorizzare sul piano della scelta politica; dall'altro, le ataviche paure dell'uomo circa i rischi per la propria sicurezza fisica, nel loro approcciarsi all'ignoto tecnologico che tali innovazioni prospettano di introdurre nella vita di tutti i giorni.

Il discorso sulla colpa penale, insomma, imbattendosi nel *novum* delle tecnologie dell'intelligenza artificiale, non fa che riproporre alcune problematiche di fondo – di matrice forse più antropologica e sociopolitica che giuridica in senso stretto – che lo caratterizzano; che già l'incontro con la modernità tecnologica – quella che in sociologia si è definita "post-modernità", o "società del rischio" – ha acuito e riproposto; e che la prospettiva ulteriore e ultima di evoluzione del contesto in cui può compiersi il reato colposo – ovvero quando ciò accada per mano di un soggetto artificiale intelligente – fa emergere in modo ancor più incisivo [8].

2.2. *Macchine intelligenti e imprevedibilità tecnologica*

Da sempre il diritto penale ha conosciuto la figura del "mezzo", o "strumento", del reato. Le "macchine", *lato sensu* intese, ne hanno finora condiviso appieno lo statuto: anche il più complesso dei computer, se utilizzato per commettere un reato, lascia inalterata la responsabilità del soggetto umano alle sue spalle, al pari del più rudimentale degli utensili di cui quest'ultimo si sia avvalso a fini criminosi [9].

Nei reati colposi, in particolare, qualora l'evento lesivo sia provocato da un

collettiva. Per tutti, nella letteratura sociologica, U. BECK, *La società del rischio. Verso una seconda modernità* (1986), Carocci, Roma, 2000, p. 38; A. GIDDENS, *Le conseguenze della modernità* (1990), Il Mulino, Bologna, 1994, p. 125; N. LUHMANN, *Sociologia del rischio* (1991), Mondadori, Milano, 1996, p. 40; nella letteratura penalistica, oltre a C. PIERGALLINI *Danno da prodotto e responsabilità penale*, cit., p. 16, v. M. DONINI, *Il volto attuale dell'illecito penale. La democrazia penale tra differenziazione e sussidiarietà*, Giuffrè, Milano, 2004, p. 107; J.M. SILVA SÁNCHEZ, *La expansión del derecho penal. Aspectos de la Política criminal en las sociedades postindustriales*, III ed., BdeF, Montevideo-Buenos Aires, 2011, p. 26; B. MENDOZA BUERGO, *El derecho penal en la sociedad del riesgo*, Civitas, Madrid, 2001, p. 24. Più in generale, sul tema del rischio, oltre già a V. MILITELLO, *Rischio e responsabilità penale*, Giuffrè, Milano, 1988, p. 55, C. PERINI, *Il concetto di rischio nel diritto penale moderno*, Giuffrè, Milano, 2010, p. 168.

[8] Sull'IA come "ultimo stadio" del percorso conflittuale della colpa nella società del rischio, C. PIERGALLINI, *Intelligenza artificiale: da "mezzo" ad "autore" del reato?*, cit., p. 1747.

[9] Per tutti: U. PAGALLO, *Saggio sui robot e il diritto penale*, cit., p. 595.

cattivo uso o da un difetto di costruzione o progettazione di un prodotto, di esso ne potrà rispondere – ove ovviamente ricorrano gli estremi della colpa – l'utilizzatore o il produttore umano [10]. La tipologia di prodotto considerato, in caso di particolare complessità del suo funzionamento, o del processo industriale in cui è costruito, al massimo potrà rendere più difficili e articolati i giudizi di causalità materiale, o – soprattutto – di colpa.

Ciò, tuttavia, non muta ancora il ruolo neutrale, silente, che la *res* assume nel fare da tramite fra il soggetto umano cui si giudica se imputare il fatto e l'accadimento lesivo stesso. Tale neutralità, infatti, si radica nella sostanziale *prevedibilità* del "comportamento" del prodotto-oggetto tradizionale. A fronte di determinate situazioni, o di determinati comandi, un prodotto – anche avente la veste di "macchina" complessa, ma non gestito da tecnologie dell'IA – reagirà sempre allo stesso modo, in base alla sua conformazione materiale o programmazione algoritmica; di talché l'uomo che lo gestisca o lo progetti è, a monte, nelle condizioni di rappresentarsi gli effetti provocati dalle proprie azioni per mezzo del prodotto stesso.

È un fatto ormai noto come il carattere "intelligente" dei soggetti artificiali che si avvalgono delle tecnologie in discussione conduca invece all'almeno parziale *imprevedibilità* del loro comportamento, a fronte di analoghi stimoli [11]. Elemento connaturato all'intelligenza artificiale, infatti, è la sua capacità di apprendimento, il *machine learning*. Esso, nel suo strutturale funzionamento, modifica i percorsi decisionali della "macchina" rispetto a quanto originariamente previsto in sede di programmazione [12].

Viene introdotta, così, un'*opacità tecnologica* al percorso imputativo tradizionale dell'evento colposo all'azione del soggetto umano che sta dietro al prodotto intelligente [13]: la "macchina" non è più un tramite neutrale, un puro mez-

[10] U. PAGALLO, *The Adventures of Picciotto Roboto: AI & Ethics in Criminal Law*, in AA.VV., *The Social Impact of Social Computing. Proceedings of the Twelth International Conference ETHICOMP 2011*, Sheffield, 2011, p. 352.

[11] S. BECK, *Google Cars, Software Agents, Autonomous Weapons Systems*, cit., p. 243; U. PAGALLO, *The Laws of Robots*, cit., p. 47.

[12] E. PALMERINI, voce *Robotica*, in E. SGRECCIA, A. TARANTINO (diretta da), *Enciclopedia di bioetica e scienza giuridica*, vol. X, ESI, Napoli, 2016, p. 1106; S. BECK, *Intelligent agents and criminal law*, cit., p. 140; I. SALVADORI, *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale*, cit., p. 102. Sul *machine learning*, cfr. H. SURDEN, *Machine Learning and Law*, in *Washington Law Review*, 2014, p. 87; J. STILGOE, *Machine learning, social learning and the governance of self-driving cars*, in *Social Studies of Science*, 2018, p. 29.

[13] H. SURDEN, M.A. WILLIAMS, *Technological Opacity, Predictability, and Self-Driving Cars*, in *Cardozo Law Review*, 2016, p. 157; Y. BATHAEE, *The Artificial Intelligence Black Box and the Failure of Intent and Causation*, in *Harvard Journal of Law & Technology*, 2018, p. 889.

zo-oggetto, ma diviene almeno in parte soggetto a carattere autonomo e proattivo. Essa è, insomma, un "prodotto soggettivizzato", che non si limita più a realizzare la volontà umana che le sta dietro, ma agisce nel mondo in modo che non è più governato integralmente dalla mano dell'uomo.

2.3. *Il "*responsibility gap*" e le problematiche regolative dell'attribuzione di colpa: i riflessi sull'imputazione ai produttori umani*

Più aumenta il carattere "intelligente" di simili prodotti, più la portata di una simile imprevedibilità tecnologica è destinata ad aumentare. Così, lo scenario prossimo è evidentemente quello di un progressivo aumento del peso di una questione che ad oggi è ancora in parte speculativa, ma che in prospettiva futura parrebbe indirizzata ad assumere un rilievo applicativo affatto trascurabile.

L'opacità tecnologica si ripercuote infatti sul meccanismo tradizionale di addebito del reato colposo d'evento: l'imprevedibilità «*paralizza il giudizio di imputazione per colpa*» [14], generando un *responsibility gap*, un *vuoto di responsabilità* [15]. Via via che i margini di autonomia dei soggetti artificiali intelligenti aumenteranno, saranno infatti sempre più i possibili risultati lesivi dell'incolumità umana, provocati dal comportamento di questi, che rimarranno privi di "copertura" sul piano della responsabilità penale.

Si può accennare, in modo schematico, gli effetti che una simile evoluzione avrebbe sulle due figure umane più tipiche – già ricordate – che vengono in rilievo in relazione ai danni cagionati da prodotto. Da un lato, l'utente, l'*utilizzatore* del prodotto stesso. Dall'altro, a monte, il suo progettatore, programmatore, manufattore: in senso lato, il *produttore*.

Iniziando da quest'ultima figura, si potrebbe dire come le indubbie più ampie difficoltà sul piano imputativo che la riguardano rendono paradossalmente più semplice lo scenario delle scelte regolative rimesse alla politica criminale. L'eventualità di imputare al produttore umano possibili accadimenti lesivi connessi all'autonomia del prodotto appare infatti così complessa da non lasciare sostanzialmente alcun margine a scelte politiche che individuino soggetti umani cui addossare la responsabilità, la "colpa", in modo da occultare il problema del *responsibility gap*.

[14] C. PIERGALLINI, *Intelligenza artificiale: da "mezzo" ad "autore" del reato?*, cit., p. 1760.

[15] B. MAGRO, *Biorobotica, robotica e diritto penale*, cit., p. 515; cfr. altresì, più in generale, P. PAGALLO, S. QUATTROCOLO, *The impact of AI on criminal law, and its twofold procedures*, in W. BARFIELD, U. PAGALLO (eds), *Research Handbook on the Law of Artificial Intelligence*, Elgar, Cheltenham-Northampton, 2018, p. 385. In una prospettiva più ampia, J. DANAHER, *Robots, Law and the Retribution Gap*, in *Ethics and Information Technology*, 2016, p. 299.

In effetti, la tipologia di eventi avversi evocata non riguarda quelle tipologie di colpa del "produttore" che si sostanziano in un difetto di manifattura, o di manutenzione [16], di vero e proprio errore nella programmazione [17], o anche di mancato aggiornamento della stessa [18]; le quali potrebbero essere ancora inquadrati secondo le (invero già assai complesse) cadenze "ordinarie" di responsabilità del produttore.

La casistica che qui rileva, piuttosto, riguarda quelle ipotesi in cui il danno derivi da un comportamento – come detto – *imprevedibile* del soggetto artificiale, attribuibile a quel margine di autonomia lui riservato, in cui è chiamata in causa la responsabilità del produttore nella persona del *programmatore*.

In tali ipotesi, se anche solo fossero superabili le difficoltà connesse all'individuazione del singolo (o dei singoli) soggetti umani responsabili all'interno di una rete plurisoggettiva di produzione-programmazione la cui estensione e complessità è ben intuibile, residuerebbe comunque il problema di fondo per cui il comportamento *imprevedibile* della macchina, come tale, per definizione non può certo essere rimproverato *per colpa* al programmatore [19]. E anche il dubbio circa il carattere più o meno prevedibile di tale azione dovrebbe far propendere per una soluzione liberatoria della figura umana astrattamente individuabile.

L'effetto complessivo, così, è che tale problematica, solo apparentemente circoscritta, peraltro installandosi in un quadro già di elevata complessità quanto all'attribuzione di colpevolezza, conduce alla sostanziale impossibilità di individuare soggetti umani la cui "colpa" possa colmare il vuoto di responsabilità di matrice tecnologica.

2.4. (Segue). *I riflessi sull'imputazione agli utilizzatori umani*

Diverso è lo scenario che riguarda la figura dell'utilizzatore umano delle tecnologie dell'IA, la quale – in ragione della sua prossimità rispetto al fatto – conserva la possibilità di essere responsabilizzata sul piano penalistico anche in ipo-

[16] Da intendersi ovviamente come esecuzione della manutenzione, rientrando la sua omissione, ove doverosa (se periodicamente richiesta, oppure al manifestarsi di un guasto o difetto prevedibilmente pericoloso) nelle eventuali responsabilità del proprietario-utilizzatore.

[17] Ad esempio, mediante inserimento di dati errati.

[18] È il caso dell'omessa considerazione di nuovi dati emersi dalla ricerca o sviluppo, oppure dalla casistica concreta (ad esempio, il verificarsi di un sinistro da parte di un soggetto IA di analogo modello).

[19] S. BECK, *Google Cars, Software Agents, Autonomous Weapons Systems*, cit., p. 244; U. PAGALLO, *The Laws of Robots*, cit., p. 72.

tesi di elevata automazione, e rimane pertanto aperta, in punto di disciplina, a subire le influenze derivanti dalla sensibilità politico-criminale sull'argomento.

In generale, la fattispecie dell'utilizzatore si caratterizza per il fatto che la "novità" rispetto al passato recente, che è data dal carattere intelligente del prodotto di cui questi fa uso, si innesta su un genere di attività che invece, tradizionalmente, era in tutto e per tutto umana (la guida su strada [20], l'attività medico-chirurgica [21], e così via).

Lo specifico fine dell'introduzione della tecnologia dell'intelligenza artificiale è evidentemente quello di affiancare, coadiuvare chi compia tale attività, permettendogli di farla con minor impegno e fatica, oppure con maggiore accuratezza, o comunque utilizzando risorse e capacità inaccessibili a un soggetto umano.

Almeno in un primo momento, un simile ausilio non è progettato per giungere a sostituire *tout court* l'uomo. Sviluppi tecnologici ulteriori, con l'approdo a un'autonomia del soggetto artificiale piena e completa, rendono possibile l'eventualità di far transitare il ruolo dell'uomo a quello di mero controllore di un'attività della "macchina" del tutto indipendente; se non addirittura a quella di mero fruitore passivo di un servizio automatizzato, privo financo della possibilità di interferire con l'azione artificiale.

[20] La letteratura penalistica sulle auto a guida autonoma, in ambito internazionale e in special modo statunitense, è sterminata. Senza la minima pretesa di completezza, per tutti: E. HILGENDORF, *Automated Driving and the Law*, in E. HILGENDORF, U. SEIDEL (eds), *Robotics, Autonomics and the Law*, Nomos, Baden-Baden, 2017, p. 171; F. DOUMA, S.A. PALODICHUK, *Criminal Liability Issues Created by Autonomous Vehicles*, in *Santa Clara Law Review*, 2012, p. 1157; J. GURNEY, *Driving into the Unknown: Examining the Crossroads of Criminal Law and Autonomous Vehicles*, in *Wake Forest Journal of Law & Policy*, 2015, p. 393; C.W. WESTBROOK, *The Google Made Me Do It: The Complexity of Criminal Liability in the Age of Autonomous Vehicles*, in *Michigan State Law Review*, 2017, p. 97. Nella letteratura italiana, L. PICOTTI, *Profili di responsabilità penale per la circolazione di veicoli a guida autonoma*, in *Studi in onore di Antonio Fiorella*, vol. I, Roma Tre Press, Roma, 2021 p. 813; sia poi consentito il rinvio, una volta per tutte, al nostro A. CAPPELLINI, *Profili penalistici delle* self-driving cars, in *Dir pen. cont.-Riv. trim.*, 2/2019, p. 325, anche per più ampi riferimenti bibliografici.

[21] Sul tema dei rapporti tra attività terapeutiche e impiego dell'IA in medicina (in ottica tuttavia prevalentemente civilistica), la letteratura è ormai ampia: per tutti, E. COLLETTI, *Intelligenza artificiale e attività sanitaria. Profili giuridici dell'utilizzo della robotica in medicina*, in *Rivista di Diritto dell'Economia, dei Trasporti e dell'Ambiente*, 2021, p. 201; Z. HARNED, M.P. LUNGREN, P. RAJPURKAR, *Machine Vision, Medical AI, and Malpractice*, in *Harvard Journal of Law & Technology Digest*, 2019; F. GRIFFIN, *Artificial Intelligence and Liability in Health Care*, in *Health Matrix: The Journal of Law-Medicine*, 2019, p. 65; in un'ottica penalistica, A. PERIN, *Standardizzazione, automazione e responsabilità medica. Dalle recenti riforme alla definizione di un modello d'imputazione solidaristico e liberale*, in *Rivista di BioDiritto*, 1/2019, p. 229.

L'esempio più immediato di tale paradigma è quello delle cosiddette auto a guida autonoma, i cui principali prototipi – ad oggi – in sviluppo presentano livelli di automazione tali da consentire una circolazione su strada in parte anche senza l'intervento diretto dell'uomo, benché ancora (almeno in Italia) sia imposta la costante sorveglianza dell'"utilizzatore"[22]. Non mancano, tuttavia, modelli ancor più avanzati, dotati di un tale livello di autonomia da poter fare a meno degli stessi comandi di guida.

Ora, fintantoché permane una figura umana di "utilizzatore" con un potere materiale di intervento, di governo, sull'azione autonoma del soggetto artificiale, tale da sovrascriverne gli schemi algoritmici e correggerne il comportamento anche "in corsa", durante il suo svolgimento, il problema del *responsibility gap* generato dalle tecnologie dell'IA rimane ancora in larga misura nascosto.

Infatti, la persistenza di un potere materiale ed effettivo di intervento dell'uomo fa scivolare la questione sul piano tutto politico di sé, come ed eventualmente in che misura sia opportuno gravare questi di un vero e proprio *obbligo giuridico* di controllo e intervento rispetto all'attività del soggetto artificiale intelligente.

Ove si ritenga in via interpretativa che un simile obbligo sussista[23], l'utilizzatore umano potrà essere ritenuto responsabile degli eventi avversi derivati dal malfunzionamento dell'IA, avendo tenuto un comportamento, *lato sensu* omissivo[24], integrante gli estremi della colpa penale. E ciò può valere – al limite – anche ove l'attività del soggetto artificiale giunga *davvero* ad essere sostanzial-

[22] Il Codice della strada italiano, al momento, non ha subito modifiche, di talché dovranno ancora ritenersi "*veicoli*" – a mente dell'art. 46 – "*tutte le macchine di qualsiasi specie, che circolano sulle strade guidate dall'uomo*". Sono pertanto da ritenersi finora ammissibili solo dei meccanismi minori di automazione, sostanzialmente di "guida assistita", tali che l'uomo permanga saldamente al governo del mezzo.

[23] Desumendolo dalle norme che attribuiscono all'utilizzatore umano il governo dell'IA (ad esempio, il citato art. 46 C.d.S. per le auto a guida autonoma). Oppure, più radicalmente, si giunga a imporlo espressamente a livello di diritto positivo.

[24] A stretto rigore, la condotta potrà dirsi omissiva, in senso proprio, solo quando nella fattispecie concreta l'autonomia dell'IA sia sostanzialmente integrale, limitandosi l'utilizzatore a sorvegliare un'attività "altrui", mentre dovrà ancora qualificarsi come commissiva quando l'uomo conservi, nella fisiologia del fenomeno, almeno in parte la necessità di "portare avanti" l'azione con ragionevole continuità, pur agevolato dal mezzo artificiale intelligente. Ma anche in tale ultimo caso, il fatto che qui interessa rimane pur sempre l'omissione del controllo e/o dell'intervento correttivo rispetto a un agire di mano del soggetto artificiale, anche se inserito in un "contesto" di azione complessivamente commissivo. Del resto, i confini tra azione commissiva e omissiva tendono a sfumare in ambito colposo, considerato il comune carattere normativo della colpa e dell'omissione, nonché la presenza di un momento omissivo in ogni condotta colposa: F. GIUNTA, *Illiceità e colpevolezza nella responsabilità colposa*, Cedam, Padova, 1993, p. 90; P. VENEZIANI, *Regole cautelari "proprie" ed "improprie" nella prospettiva delle fattispecie colpose causalmente orientate*, Cedam, Padova, 2003, p. 44.

mente autonoma – ovvero senza necessità di intervento pratico, anche solo saltuario, dell'utilizzatore – ma tuttavia permanga, anche solo in astratto, la possibilità di intervento sostitutivo dell'uomo.

Lo scenario muta soltanto dove – come accennato – la tecnologia utilizzata raggiunga un livello di sviluppo tale da escludere del tutto la stessa materiale possibilità di intervento dell'uomo: si pensi all'ipotesi di un *robotaxi* con clienti che, come in tutti i taxi, siano meri passeggeri, o comunque a vetture private a guida autonoma prive del volante e dei pedali, il cui proprietario non possa definirsi conducente ma anch'egli – appunto – mero passeggero.

In tale prospettiva-limite, il *responsibility gap* si mostra senza veli: venendo meno la possibilità di imputare un eventuale risultato lesivo a un utilizzatore che non partecipa più in alcun modo dell'azione pericolosa, addirittura ormai privato della capacità di governarla, non rimane nient'altro che un problematicissimo "fatto proprio" del soggetto artificiale. Oppure – dipende dai punti di vista – un caso fortuito: un fatto che la vittima subisce, senza che vi sia la possibilità di attribuirne la responsabilità a qualcuno, e che rimane pertanto un frutto della casualità.

2.5. *IA, colpa, caso fortuito: la politicità della soglia del rischio consentito e le influenze della precauzione*

In un simile scenario, non sorprende come le "ragioni" della nuova tecnologia dell'IA non siano le sole a giocare un ruolo di primo piano in quel complesso e articolato giudizio politico di bilanciamento tra interessi che individua, a livello sociale prima e giuridico poi, la soglia del rischio consentito, ripartendo le aree da un lato del caso fortuito (o, che dir si voglia, del "fatto" che ricade solo sulla vittima) e, dall'altro, dell'attribuibilità a qualcuno per colpa.

Ciò accade nonostante, su un piano strettamente oggettivo, siano vari e validi gli argomenti che depongono in favore di una politica quanto più ampia possibile di autorizzazione di simili tecnologie e di sollevazione degli utenti dalle responsabilità penali conseguenti al loro maneggio. Statisticamente parlando, in effetti, si potrebbe dire come le "macchine" – già adesso – siano spesso *più sicure* della mano dell'uomo che mirano a sostituire.

Anzitutto, c'è da dire che, se a livelli di automazione più basilari la sorveglianza e l'eventuale intervento umano possono ancora garantire dei livelli di sicurezza oggettivamente più elevati, a stadi tecnologici più avanzati l'interferenza umana può rivelarsi addirittura pericolosa, se non essa stessa possibile autonoma fonte di incidenti.

Più la macchina è capace di fare da sé, più il controllo umano si riduce ad

impedire una prospettiva, sempre più improbabile e remota, di malfunzionamento. Ma allora, in certi casi saranno inevitabili i cali di attenzione e di prontezza dell'utilizzatore umano in un contesto di prolungata mera sorveglianza passiva (si pensi al settore, ancora, delle macchine a guida autonoma [25]). Similmente, è irrealistico pensare che un uomo sempre più disabituato a compiere da solo le attività in questione sia efficacemente in grado di intervenire proprio in momenti di crisi, a elevata difficoltà [26]. E ancora, rispetto ad altri settori di attività (ad esempio, in campo medico), è irrealistico immaginare che l'uomo possa davvero sopperire al soggetto artificiale dove il *quid pluris* di quest'ultimo sia una precisione o accuratezza fisiologicamente impossibili per la mano umana.

Poi, rimane sempre il problema della riconoscibilità, da parte del controllore, dell'"avaria", del momento in cui è necessario intervenire. È facile immaginare come la difficile "leggibilità" del comportamento artificiale agli occhi umani possa condurre a interventi correttivi – istintivi, dettati da paura, o altro – non necessari o errati, talvolta essi stessi forieri di pericolo [27].

Ma anche al di là della sostanziale inefficacia oggettivo-preventiva della sorveglianza umana, va infine considerato come la *ratio* stessa dell'innovazione tecnologica, in molti settori, verrebbe sostanzialmente frustrata ove la figura umana conservasse una responsabilità *omnibus* per l'attività artificiale. Ciò non consentirebbe, nella sostanza, il minimo sgravio di impegno per l'uomo, limitandosi a trasformare un dovere di attenzione nell'esecuzione proattiva di un'attività pericolosa in un non meno capillare e continuo dovere di controllo rispetto al compimento di un'azione "altrui".

Eppure, il carattere – come detto – tutto politico della questione fa sì che gli argomenti ripercorsi siano solo alcuni di quelli che entrano davvero in gioco nella scelta regolativa circa fino a che punto consentire l'utilizzo pubblico di soggetti artificiali intelligenti e – soprattutto – *se* e *in che misura* esonerare da responsabilità gli utilizzatori umani – gli unici soggetti, come visto, davvero strutturalmente capaci di caricarsi della "colpa" – non imponendo loro un obbligo di controllo onnicomprensivo.

Non si può non tenere conto, infatti, del ruolo capitale che la paura dell'ignoto tecnologico ha nel determinare le scelte compiute a livello regolativo, e in

[25] E. ARIA, J. OLSTAM, C. SCHWIETERING, *Investigation of Automated Vehicle Effects on Driver's Behaviour and Traffic Performance*, in *Trasportation Research Procedia*, 2016, p. 761.

[26] F. DOUMA, S.A. PALODICHUK, *Criminal Liability Issues Created by Autonomous Vehicles*, cit., p. 1164.

[27] A. HEVELKE, J. NIDA-RÜMELIN, *Responsibility for Crashes of Autonomous Vehicles: An Ethical Analysis*, in *Science and Engineering Ethics*, 2015, p. 624; J. GURNEY, *Driving into the Unknown*, cit., p. 416.

particolare del potere di piegarle a logiche ispirate a criteri, anche estremi, di precauzione [28].

In ogni società l'imputazione di un evento avverso a taluno, l'individuazione di un colpevole, svolge un ruolo di rassicurazione del gruppo collettivo. È un esorcismo antropologico-giudiziario il quale, così spiegando il verificarsi di una sciagura, dà conto del fatto che essa si è verificata per "colpa" di qualcuno, presupponendo che senza tale "colpa" nulla di tragico sarebbe accaduto, e che la realtà avrebbe preservato intatta la sua illusione di sicurezza [29]. Senza la spiegazione data dell'attribuzione di "colpa", invece, quell'evento, quel male, diventa il frutto beffardo del caso, privo di spiegazioni, indominabile: come tale, fonte di angoscia per l'uomo [30].

Tale atteggiamento, intimamente connesso alla natura umana più profonda, nel confronto storico con nuove tecnologie e correlati pericoli tende a perpetuarsi individuando – quando non sia possibile neutralizzare i nuovi rischi con divieti *tout court* – potenziali colpevoli cui addossare gli inevitabili conseguenti risultati di danno, rifuggendo così il timore connesso al vuoto di responsabilità [31].

Nel caso delle tecnologie dell'IA, pertanto, sulla falsariga di quanto appena detto, il rischio tangibile è dunque duplice. Anzitutto, quello di attendismo, in particolare con riferimento al consentire l'utilizzo di quei soggetti artificiali con livelli di autonomia particolarmente elevati, nelle scelte regolatorie che i singoli Stati sono chiamati a compiere in merito alla portata e ai limiti che simili tecnologie riscontreranno nel mercato; con evidente pregiudizio dei benefici che pure le stesse prospettano all'uomo.

[28] Sul principio di precauzione in ambito penalistico, per tutti: D. CASTRONUOVO, *Principio di precauzione e diritto penale: paradigmi dell'incertezza nella struttura del reato*, Aracne, Roma, 2012; G. FORTI, *"Accesso" alle informazioni sul rischio e responsabilità: una lettura del principio di precauzione*, in *Criminalia*, 2006, p. 155; F. GIUNTA, *Il diritto penale e le suggestioni del principio di precauzione*, in *Criminalia*, 2006, p. 227.

[29] La letteratura extragiuridica sul punto è sterminata. Per tutti, M. DOUGLAS, *Purezza e pericolo. Un'analisi dei concetti di contaminazione e tabù* (1970), Il Mulino, Bologna, 2014; ID., *Rischio e colpa* (1992), Il Mulino, Bologna, 1996; F. REMOTTI, *Maleficio*, in P.P. PORTINARO (a cura di), *I concetti del male*, Einaudi, Torino, 2002, p. 148; Z. BAUMAN, *Paura liquida*, Laterza, Roma-Bari, 2006, p. 69; W. SOFSKY, *Rischio e sicurezza*, Einaudi, Torino, 2005, p. 12.

[30] In dettaglio, nella letteratura penalistica, D. CASTRONUOVO, *La colpa penale*, Giuffrè, Milano, 2009, p. 86.

[31] L. STORTONI, *Angoscia tecnologica ed esorcismo penale*, in *Riv. it. dir. proc. pen.*, 2004, p. 71; F. STELLA, *Giustizia e modernità. La protezione dell'innocente e la tutela delle vittime*, III ed., Giuffrè, Milano, 2003, p. 552; F. CENTONZE, *La normalità dei disastri tecnologici. Il problema del congedo dal diritto penale*, Giuffrè, Milano, 2004, p. 35; G. CIVELLO, *La "colpa eventuale" nella società del rischio. Epistemologia dell'incertezza e "verità soggettiva" della colpa*, Giappichelli, Torino, 2013, p. 197.

Ma soprattutto, è evidente il rischio di scelte politiche "ultraresponsabiliste", volte a prorogare il ruolo e i doveri di controllo ad ampio spettro, sussistenti in capo a utilizzatori umani, in maniera del tutto irrealistica: considerato come, in un simile contesto, è palese come gli stessi abbiano ormai perduto il reale governo dell'attività in questione. E ciò, sia con potenziali derive – sul piano penalistico – di inammissibili responsabilità oggettive, da posizione (*rectius*, da prossimità, *ictu oculi* evidente, al pericolo); sia – più in generale – ostacolando i benefici per l'uomo connessi a tali tecnologie, la cui diffusione viene evidentemente disincentivata da simili politiche.

2.6. *Riflessioni conclusive: quali prospettive per il futuro?*

Come detto, il timore di vuoti di tutela per i beni primari della vita, sicurezza e salute umana può ben alimentare la permanenza di politiche precauzionistiche e ultraresponsabiliste a danno dei protagonisti umani più immediatamente coinvolti, gli utilizzatori. Così, a fronte di tale problema, allo stato apparentemente irrisolvibile, è immediato interrogarsi circa le prospettive – non certo di superamento, ma quantomeno di mitigazione – di tali criticità, che potrebbero, in futuro, essere esplorate.

La via indubbiamente più suggestiva, all'apparenza fantasiosa ma – in particolare in prospettiva futura – forse non poi così tanto, è quella dell'introdurre delle forme di responsabilità dirette del soggetto artificiale, ponendo in dubbio l'assioma, finora incontestato, per il quale *machina delinquere non potest*. È una prospettiva con tutta evidenza non immediatamente percorribile nelle sue forme più radicali, giacché le macchine di oggi non posseggono ancora quella "libertà del volere" che è il presupposto di un giudizio di colpevolezza, facendo perdere così di significato e di efficacia una pena criminale che sia loro comminata, ed eventualmente irrogata, in caso di integrazione dell'illecito [32].

[32] Nella letteratura internazionale, la principale voce favorevole alla configurabilità di una responsabilità penale diretta dell'IA è G. HALLEVY, *Liability for Crimes Involving Artificial Intelligence Systems*, Springer, Dordrecht, 2015; *Virtual Criminal Responsibility*, in *Original Law Review*, 2010, p. 6; *"I, Robot – I, Criminal" – When Science Fiction Becomes Reality: Legal Liability of AI Robots committing Criminal Offences*, in *Syracuse Science & Technology Law Reporter*, 2010, p. 1. Scettica la letteratura assolutamente prevalente. Sul tema, per tutti, M. HILDEBRANDT, *Ambient Intelligence, Criminal Liability and Democracy*, in *Criminal Law and Philosophy*, 2008, p. 163; P. ASARO, *A Body to Kick, but Still No Soul to Damn: Legal Perspectives on Robotics*, in P. LIN, K. ABNEY, G.A. BEKEY (eds), *Robot Ethics*, Mit Press, Cambridge (Massachusetts), 2012, p. 169; P.M. FREITAS, F. ANDRADE, P. NOVAIS, *Criminal Liability of Autonomous Agents: From the Unthinkable to the Plausible*, in P. CASANOVAS, U. PAGALLO, M. PALMIRANI, G. SARTOR (eds), *AI Approaches to the Complexity of Le-*

Tuttavia – oltre a non chiudere la porta ad eventuali sviluppi tecnologici futuri, in realtà non del tutto prevedibili, che potrebbero condurre alla creazione di IA ancor più simili all'uomo – la riflessione può forse già oggi utilmente svolgersi, agganciandosi a una prospettiva che sia diversa da quella della penalità "classica": la quale è inevitabilmente legata, ancora oggi, ai concetti di colpevolezza e retribuzione.

La storia, invero, ha conosciuto in epoche preilluministiche delle penalità diverse – degli *animali* prima di tutto, ma anche delle *cose* – che evidentemente assolvevano a funzioni del tutto differenti rispetto a quella di punire il male, liberamente commesso, attraverso un analogo male [33]. Si trattava, probabilmente, di funzioni sinceramente *vendicatorie*, di vera e propria rappresaglia; ma anche – sotto altro angolo visuale – *consolatorie*, nella misura in cui miravano a ristorare la vittima del dolore subito, mostrando plasticamente, attraverso la natura *lato sensu* rituale, solenne, della giurisdizione penale, la solidarietà della comunità di fronte all'evento nefasto, al ricadere di un male in capo a un proprio membro [34].

Analogamente, si è suggerito da parte di alcuni come l'esercizio di una "punizione" nei confronti delle macchine che abbiano cagionato un male possa in qualche modo apportare un beneficio psicologico alla vittima (o alle persone a lei vicine), dando voce alla loro irrazionale brama di vendetta [35]. Si tratterebbe –

gal Systems, Springer, Berlin-Heidelberg, 2014, p. 145; D. LIMA, *Could AI Agents Be Held Criminally Liable? Artificial Intelligence and the Challanges for Criminal Law*, in *South Carolina Law Review*, 2018, p. 677; M. SIMMLER, N. MARKWALDER, *Guilty Robots? – Rethinking the Nature of Culpability and Legal Personhood in an Age of Artificial Intelligence*, in *Criminal Law Forum*, 2019, p. 1; R. ABBOTT, A. SARCH, *Punishing Artificial Intelligence: Legal Fiction or Science Fiction*, in *University of California Davis Law Review*, 2019, p. 323; M.A. LEMLEY, B. CASEY, *Remedies for Robots*, in *The University of Chicago Law Review*, 2019, p. 1311; N. OSMANI, *The Complexity of Criminal Liability of AI Systems*, in *Masaryk University Journal of Law and Technology*, 2020, p. 53. Cfr. altresì – nella letteratura italiana – l'ampia trattazione del tema a penna di C. PIERGALLINI, *Intelligenza artificiale: da "mezzo" ad "autore" del reato?*, cit., p. 1764.

[33] Sul tema, per tutti, cfr. il classico E.P. EVANS, *The Criminal Prosecution and Capital Punishment of Animals* (1906), trad. it. *Animali al rogo*, Res Gestae, Milano, 2012.

[34] Si tratterebbe di una sorta di versione primigenia della moderna prevenzione generale positiva. O, forse, di una sua declinazione – legata alla forza del *rito*, della gestualità sociale – che, in modo sotterraneo, ha invero sempre pervaso la penalità. In questo senso, essa potrebbe svolgersi, un domani, anche nei confronti di potenziali "autori artificiali intelligenti", offrendo ristoro alle vittime di questi.

[35] C. MULLIGAN, *Revenge Against Robots*, in *South Carolina Law Review*, 2018, p. 579. Non si è mancato tuttavia di contestare simili impostazioni, su un piano anzitutto etico, ritenendo che istituzionalizzare simili "vendette" educherebbe alla violenza, con il rischio che questa finisca per coinvolgere anche vittime umane: K. DARLING, *Extending Legal Pro-*

ci pare – di una sorta di penalità "decolpevolizzata", intermedia tra la (ritualmente neutra) gestione amministrativa di interessi e la penalità classica, colpevole: costituzionalmente possibile, nei confronti delle "macchine", perché non ancora soggetti di diritto al pari dell'uomo, dunque "sacrificabili" anche in mancanza di colpevolezza allo specifico fine di apportare un beneficio a un soggetto di diritto "pieno".

Un'altra via, certamente un po' più immediata, che potrebbe valer la pena esplorare è quella della responsabilità da reato dei soggetti collettivi [36]. Dietro ogni IA c'è infatti inevitabilmente una società commerciale che riassume l'insieme delle competenze tecnico-specialistiche necessarie a "tenere in piedi" progetti di sviluppo e produzione così complessi. La natura collettiva di tale soggetto, peraltro, parrebbe permettere di bypassare il problema altrimenti insolubile – poc'anzi evocato – dell'individuazione dei singoli programmatori, nell'enorme rete plurisoggettiva del circuito di produzione, che non hanno previsto ciò avrebbero dovuto prevedere. Il nome del "colpevole" si ritroverebbe, banalmente, inciso sulla carrozzeria del soggetto robotico…

Le cose, tuttavia, sono più complesse di quanto simili tentazioni semplificatorie facciano sperare. Certamente, un errore di programmazione – non univocamente riconducibile a singoli soggetti determinati – potrà ben essere attribuito alla responsabilità dell'ente quando lo stesso si radichi in un deficit organizzativo del soggetto collettivo: una *colpa* della *corporation* che, così, rimpiazzi l'impraticabile colpa penale del singolo. Ciò, tuttavia, non elimina affatto il problema principale: il *responsibility gap*. *Il comportamento imprevedibile della macchina*, come tale, *è e rimane non imputabile anche all'ente*: la cui colpevolezza si deve radicare in una mancanza organizzativa relativa a dei rischi che siano comunque *prevedibili ex ante*.

Insomma: la responsabilità da reato degli enti sarà sì uno strumento indispensabile della *governance* pubblica dei prodotti IA (a fianco di quello risarcitorio e, ovviamente, di quello strettamente amministrativo, regolatorio/sanzionatorio)

tection to Social Robots: The Effects of Antropomorphism, Emphaty, and Violent Behaviour Towards Robotic Objects, in R. CALO, A.M. FROOMKIN, I. KERR (eds), *Robot Law*, Elgar, Cheltenham-Northampton (Massachusetts), 2016, p. 213; *contra*, P. SWEENEY, *Why Indirect Harms do not Support Social Robot Rights*, in *Minds & Machines*, 2022.

[36] Sull'implementazione di una "responsabilità 231" per i fatti colposi commessi da IA, sia sotto un profilo dogmatico che politico-criminale, C. PIERGALLINI, *Intelligenza artificiale: da "mezzo" ad "autore" del reato?*, cit., p. 1753. Cfr. altresì FED. MAZZACUVA, *The Impact of AI on Corporate Criminal Liability: Algorithmic Misconduct in the Prism of Derivative and Holistic Theories*, in G. VERMUELEN, N. PERŠAK, N. RECCHIA (eds), *Artificial Intelligence, Big Data and Automated Decision-Making in Criminal Justice*, Maklu, Antwerpen, 2021, p. 143; DIAMANTIS M.E., *The Extended Corporate Mind: When Corporations Use AI to Break the Law*, in *North Carolina Law Review*, 2020, p. 893.

per correggere molte carenze e difetti sul piano dell'organizzazione, programmazione e produzione. Essa, tuttavia, risulta al contempo insufficiente a fornire una copertura di tutela, con finalità strettamente *preventive*, in relazione a *tutti* i rischi: e in particolare a quelli – massimamente problematici – di derivazione tecnologica.

E in ogni caso, anche volendo mettere da parte una simile insufficienza sul piano della prevenzione, residua comunque il diverso problema sopra accennato: ovvero se l'alternativa della responsabilità collettiva fornisca un valido sostituto all'imputazione del singolo sotto il diverso angolo visuale della necessità di *rassicurazione sociale*, di irrazionale esorcismo collettivo, connessa all'evento avverso di matrice tecnologica. Può una sanzione sostanzialmente pecuniaria all'ente surrogare la classica penalità individuale, con la sua "rassicurante" definitività nel "dare le colpe" e spiegare, così, il perché dell'evento avverso?

È un interrogativo aperto, cui forse si è istintivamente portati a dare risposta del tutto negativa, lasciando così irrisolto il *responsibility gap*; ma che, al contrario, meriterebbe probabilmente un più approfondito esame, al pari dei molti altri interrogativi che popolano un'area di frontiera solo apparentemente lontana e futuristica.

CAPITOLO III

Note sparse sull'intelligenza artificiale

ANDREANA ESPOSITO

SOMMARIO: 3.1. A mo' di introduzione. – 3.2. Prevedere il futuro. – 3.3. *Compliance* predittiva. – 3.3.1. Il caso dell'antiriciclaggio. – 3.4. Per concludere.

3.1. *A mo' di introduzione*

Il presente scritto è una breve riflessione intorno alla Intelligenza artificiale [1], tema da me scarsamente praticato, che ho per lo più seguito a distanza, considerandolo poco attraente, se non addirittura arido. Avvicinatami con cautela, ho iniziato a esplorare la complessità di cui lo stesso si compone e ho, finalmente, iniziato a "vedere", a capire quanto l'IA sia una entità dinamica, esuberante, straripante e come abbia oramai permeato qualsiasi ambito cognitivo e/o sociale.

Viviamo nella rete. Intorno a noi vi sono battaglioni di algoritmi intelligenti in continua e silenziosa attività [2]. Noi non li vediamo, ma loro ci osservano, ci

[1] L'AI, o in italiano, IA, è acronimo di Intelligenza artificiale usato per indicare la capacità delle macchine di risolvere problemi. La prima volta che questa espressione è stata utilizzata in questo senso è con il *Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, presentato al Dartmouth College nel 1956 da John McCarthy e altri. Il documento è consultabile su: *http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf*., trad. in italiano, *Proposta di un Progetto di ricerca estivo sull'intelligenza artificiale presso il Dartmouth College*, in *Sistemi intelligenti*, XVIII, 2006, p. 413 ss. Per una definizione in contesto normativo ed europeo, cfr. Comunicazione della Commissione europea, *L'intelligenza artificiale per l'Europa*, COM (2018) 237, del 25 aprile 2018. Per ulteriori e puntuali rinvii bibliografici nonché disamina del tema, cfr. F. BASILE, *Intelligenza artificiale e diritto penale: qualche aggiornamento e qualche nuova riflessione*, in questo Volume p. 1 ss. e, anche, F. BASILE, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Dir. pen. uomo*, 2019.

[2] A seconda del livello di autonomia e di indipendenza che possiedono rispetto allo sviluppatore, in scala crescente di indipendenza è possibile distinguere tra algoritmi determini-

imitano e fanno esperimenti su di noi. Analizzano i nostri comportamenti *online* per intercettare i nostri gusti, anche quelli che sono nel nostro inconscio; esaminano e controllano il nostro stato di salute; frugano nei nostri conti correnti e nei nostri debiti stimando la nostra solvibilità; misurano e dicono di prevedere la nostra pericolosità come potenziali criminali; soppesano la nostra efficienza come lavoratori. In sintesi: il mondo dell'intelligenza artificiale è quello in cui lavoriamo, impariamo, viaggiamo. In cui viviamo.

Addentrandomi nel mondo della tecnologia e del tecno diritto [3] sono stata letteralmente sommersa da una letteratura sterminata, impossibile per una mente umana da controllare [4]. Mi sono persa in mezzo agli infiniti *input*, alla quantità ingovernabile di parole e di concetti, alle tante storie di rapporti tra macchine con nomi umani, le *chatbo*t: Parry ed Eliza (lo psicopatico e la sua dottoressa) [5], Bob e Alice (i ribelli che hanno iniziato a usare tra loro un linguaggio incomprensibile), perdendomi in un vortice sempre più incontenibile che faticavo a gestire.

Fino a quando sono inciampata nell'*Algoritmo definitivo*.

L'*Algoritmo definitivo*, titolo di un libro di Pedro Domingos [6], scienziato di punta nello studio dell'intelligenza artificiale, mi ha prima di tutto inquietato. E l'inquietudine è aumentata leggendo le prime pagine del testo in cui l'autore,

stici (M HILDEBRANDT, *Smart Technologies and the End of Law(s)*, Edward Elgar Publishing, 2015, p. 22); algoritmi di *machine learning*, algoritmi che danno vita a sistemi multi-agente (M HILDEBRANDT, *Smart Technologies*, p. 23) e algoritmi cd. definitivi (P. DOMINGOS, *L'algoritmo definitivo*, Bollati Boringhieri, Torino, 2016).

[3] Parla di *tecno diritto* N. LETTIERI*, Antigone e gli algoritmi*, Mucchi editore, Modena, 2020.

[4] Non ho pretese di esaustività nelle indicazioni bibliografiche. Al contrario. Mi limiterò, pertanto, a indicare alcune letture che ho trovato utili e facilitanti la comprensione del tema che è trattato nel presente Volume. Così, tra gli altri, per una disamina sull'evoluzione storica dell'IA, T. NUMERICO, *Big date e algoritmi*, Carocci Editore, Roma, 2021, in particolare p. 25 ss.; C. FONTANA, *Definizioni e lineamenti tecnici essenziali dell'intelligenza artificiale: cenni al quadro regolamentare e ai principali problemi giuridici*, in G.C. FERRONI, C. FONTANA, E.C. RAFFIOTTA (a cura di), *AI Anthology, Profili giuridici, economici e sociali dell'intelligenza artificiale*, Il Mulino, Bologna, 2022, p. 65 ss., spec. p. 69 ss.; G.F. ITALIANO, *Le sfide interdisciplinari dell'intelligenza artificiale*, in *Analisi giuridica dell'economia,* 2019, p. 9 ss. Per maggiori approfondimenti, P. MCCORDUCK, *Machines Who Think. A Personal Inquiry into the History and Prospects of Artificial Intelligence*, A.K. Peters, 2004.

[5] Alla fine degli anni '60 cominciarono a svilupparsi dei *software* – cd. *chatbots* – che permettevano al dispositivo di simulare una conversazione con gli esseri umani. Uno di questi dispositivi di nome Eliza, fu inventato da Roger Weizenbaum e riproduceva il comportamento di uno psicoterapeuta di impostazione rogersiana; su questo cfr. T. NUMERICO, *Big date e algoritmi*, cit., p. 33 ss.

[6] P. DOMINGOS, *L'algoritmo definitivo*, Bollati Boringhieri, Torino, 2016.

dopo aver illustrato nel dettaglio come ogni singolo attimo della nostra esistenza sia condizionato e dipendente dagli algoritmi, scrive seguendo una progressione fanta-onirica «*Il machine learning è l'ultimo capitolo di una saga lunga milioni di anni: è lo strumento che consente alla realtà di capire cosa vogliamo e cambiare di conseguenza prima ancora che alziamo un dito. Il mondo intorno a noi – oggi virtuale, domani fisico – si modifica come una foresta magica nell'istante stesso in cui lo attraversiamo. Il cammino che scegliamo tra gli alberi e i cespugli si trasforma in una strada. Là dove ci siamo smarriti spuntano cartelli che ci indicano la strada*» [7]. Quella tracciata sembra essere paragonabile a una realtà distopica.

Foresta magica, alberi e cespugli che diventano strada magari asfaltata, cartelli che spuntano nel bosco. Continuando la lettura, ho alla fine raggiunto il punto: «*Ognuna di queste tecnologie apparentemente magiche funziona perché tutto, nel* machine learning*, ruota intorno alla capacità di prevedere*» [8].

3.2. *Prevedere il futuro*

Eccolo il punto: la prevedibilità del futuro. L'algoritmo *predittivo* – quello su cui mi soffermerò in questo mio breve e poco articolato discorso – ci affascina tanto perché ci consente (ci promette) di *conoscere* il futuro e, attraverso la conoscenza, controllare il dispiegarsi degli eventi. O almeno, così ci illudiamo.

Niente di nuovo in generale, niente di nuovo per noi giuristi. Niente di nuovo per la saggezza popolare: si pensi al detto "rosso di sera, bel tempo si spera", frase che tratta dell'osservazione del colore del cielo in un particolare momento del giorno per predire che tempo fa il giorno dopo. In questa frase è condensato il funzionamento dell'apprendimento automatico – il *machine learning* – e troviamo rappresentata l'esperienza maturata in secoli di osservazioni che utilizza una serie di caratteristiche dell'ambiente. "Rosso di sera bel tempo si spera" è un modello statistico generato dall'osservazione di dati dalla realtà, usato per fare predizioni.

Niente di nuovo per il giurista, ho detto; giurista che è sempre più ossessionato dalla necessità di prevedere il risultato di processi decisionali [9].

[7] P. DOMINGOS, *L'algoritmo definitivo*, cit., p. 15.

[8] P. DOMINGOS, *L'algoritmo definitivo*, cit., p. 16.

[9] Sull'uso degli strumenti digitali nel processo (civile, penale e amministrativo), nella letteratura italiana, v. l'ampia trattazione in R. GIORDANO, A. PANZAROLA, A. POLICE, S. PREZIOSI, M. PROTO (a cura di), *Il diritto nell'era digitale. Persona, Mercato, Amministrazione, Giustizia*, Giuffrè Francis Lefebvre, Milano, 2022.

Si pensi alla giustizia predittiva [10] o alla necessità di prevedere (calcolare, pesare) il rischio di realizzazione di reati nei tanti casi di responsabilità delle persone giuridiche [11].

La prevedibilità come certezza del diritto è una ossessione del passato che continua nel presente: dalla "macchina" di Montesquieu del giudice come *bocca della legge* alimentata da un sillogismo perfetto al diritto scientifico, matematico, geometrico, calcolabile il passo è breve. Il mito della Dea Ragione degli illuministi si è attualizzato nella giustizia predittiva, alla ricerca di una entità (in origine era un giudice, oggi è *un software*) in grado di rendere una decisione – *output* a seguito dell'inserimento di un fatto della vita – *input*. In particolare, secondo le diverse declinazioni della giustizia predittiva attraverso l'uso di *big data* [12], sterminati assembramenti di informazioni e di dati che una mente umano non è in grado di ritenere ed elaborare per quantità e qualità, si potrebbe portare ordine e regolarità laddove regna il disordine e la causalità. La potenza dell'algoritmo è infatti in grado di *masticare*, *digerire* e metabolizzare dettagli, elementi fattuali e giuridici, di milioni di casi già decisi in precedenza, prevedendo il risultato della questione giuridica con un elevatissimo grado di accuratezza [13]. I dati sono analizzati con l'aiuto di algoritmi di *deep learning* [14], metodi per re-

[10] Con il termine *giustizia predittiva* si intende quell'insieme di strumenti di supporto alla funzione giurisdizionale, in grado di analizzare in rapida sequenza una grande quantità di informazioni con l'obiettivo di prevedere l'esito di un giudizio, in proposito cfr., tra i tanti, A. SIGNORELLI, *La prevedibilità delle e nella decisione giudiziaria*, in *Il diritto nell'era digitale*, cit., p. 997 ss.; S. DE LA OLIVA, *"Giustizia predittiva", interpretazione matematica delle norme, sentenze robotiche e la vecchia storia del "justizklavier"*, in *Rivista trimestrale di diritto processuale civile*, 2019, p. 838 ss.; K.D. ASGLEY, *Artificiale Intelligence and Legal Analytics, New Tools for Law Practice in the Digital Age*, Cambridge University Press, Cambridge, 2017; M. NUZZO, *Il problema della prevedibilità delle decisioni: calcolo giuridico secondo i precedenti*, in A. CARLEO (a cura di), *Calcolabilità giuridica*, Il Mulino, Bologna, 2017.

[11] Sulle questioni sollevate dall'intelligenza artificiale nel campo giuridico, cfr. A. CARLEO (a cura di), *Decisione robotica*, Il Mulino, Bologna, 2019; anche A. GARAPON, J. LASSÉGUE, *Justice digitale. Révolution graphique et rupture anthropologique*, Presses Universitaires de France, 2018.

[12] I *big data* sono insieme di dati che crescono nel tempo, sia qualitativamente che quantitativamente. La loro raccolta può essere realizzata presso gli utenti da sensori connessi alla reta o da qualsiasi altro oggetto dell'*Internet of Things*, così in *Dizionario Legal tech*, G. ZICCARDI, P. PERRI (a cura di), Giuffrè Francis Lefebvre, Milano, 2020; sul tema, cfr. M. DEL MASTRO, A. NICITA, *Big data. Come stanno cambiando il nostro mondo*, Il Mulino, Bologna, 2019.

[13] Così, C.V. GIABARDO, *Il giudice e l'algoritmo (in difesa dell'umanità del giudicare)*, in *Giustizia insieme*, 9 luglio 2020.

[14] Sul *deep learning*, cfr. T. NUMERICO, *Big date e algoritmi*, cit., p. 134 ss. Per una sinte-

perire schemi e modelli che possono essere generalizzati e usati per fare delle previsioni per il comportamento futuro delle serie analizzate. Sono usati in diversi settori scientifici. In ambito giuridico, attraverso la lettura e l'analisi semantica di precedenti decisioni, tutte inglobate dall'algoritmo, si prova a costruire una decisione robotica [15]. Dati, dati e ancora dati: attraverso la loro combinazione si arriva a una conoscenza *sovraumana* condotta scientificamente. Non si cerca attraverso la costruzione dell'algoritmo di sostituire il processo mentale che dovrebbe essere svolto dall'interprete umano, ma sulla base della combinazione di informazioni, parole e altri parametri si costruiscono dei modelli che dovrebbero essere in grado di indicare la probabilità di certe soluzioni [16]. Sono note alcune simulazioni dell'uso, di simulazione di decisioni giudiziarie, di strumenti predittivi: dalla ricerca svolta presso l'Università College di Londra con l'elaborazione di un algoritmo in grado di prevedere in anticipo l'esito di ricorsi presentati alla Corte europea dei diritti umani (algoritmo che ha previsto le conclusioni dei giudici europei nel 79% dei casi) [17] alla creazione, sempre da parte

si dei diversi strumenti di intelligenza artificiale, cfr. N. ABRIANI, G. SCHNEIDER, *Diritto delle imprese e intelligenze artificiali*, Il Mulino, Bologna, 2021, p. 21 ss.

[15] Sulla natura giuridica da attribuire alle decisioni giuridiche conseguenti a indicazioni dell'intelligenza artificiale (se, in particolare, debbano essere considerati atti o fatti giuridici), cfr. N. ABRIANI, G. SCHNEIDER, *Diritto delle imprese*, cit., p. 51 ss.

[16] Su questi temi, tra gli altri, M. TARUFFO, *Judicial Decisions and Artificial Intelligence*, in *Artificial Intelligence and Law*, 1998, p. 316 ss.; F. ROUVIÈRE, *Le raisonnement par algorithmes: le fantasme du juge-robot*, in *Revue trimestrielle de droit civil*, 2018, p. 530 ss.; O. DI GIOVINE, *Il "judge-bot" e le sequenze giuridiche in materia penale (intelligenza artificiale e stabilizzazione giurisprudenziale)*, in *Cassazione penale*, 2020, p. 952 ss.; M. CATERINI, *Il giudice penale robot*, in *La legislazione penale*, 19 dicembre 2020. Si rinvia, anche a F. BASILE, *Intelligenza artificiale*, in questo Volume.

[17] L'algoritmo elaborato dai ricercatori dell'University College of London (UCL), prendendo in esame 584 decisioni della Corte europea, ha *valutato* la possibilità di violazione degli artt. 3, 6 e 8 della Convenzione, in materia di trattamenti disumani, giusto processo e tutela della vita privata. Ovviamente, la previsione è stata basata non su un ragionamento giuridico ma in base a un trattamento statistico dei dati raccolti, consistenti in fatti, circostanze ricorrenti, frasi più frequentemente rinvenibili e ha predetto la soluzione corretta (cioè coincidente con quella dei giudici) nel 79% dei casi, cfr. N. ALETRAS, D. TSARAPATSANIS, D. PREOŢIUC-PIETRO, V. LAMPOS, *Predicting judicial decisions of the European Court of Human Rights: a Natural Language Processing perspective*, in *PeerJ computer science*, 24 ottobre 2016, *https://peerj.com/articles/cs-93/*; e C. BARBARO, *Uso dell'intelligenza artificiale nei sistemi giudiziari: verso la definizione di principi etici condivisi a livello europeo? I lavori in corso alla Commissione europea per l'efficacia della giustizia (CEPEJ) del Consiglio d'Europa*, in *Questione giustizia*, 2018, p. 189 ss. Successiva simulazione è quella effettuata da I. CHALKIDIS, I. ANDROUTSOPOULOS, N. ALETRAS in *Neural Legal Judgment in English*, in *Association for Computational Linguistics*, 2019, p. 4317 ss. Questo secondo studio

di un gruppo di ricercatori inglesi, questa volta dell'Università di Cambridge, di un *software*, *Case Cruncher Alfa* (cioè *il masticatore di casi*) che ha vinto una gara ingaggiata con un squadra di avvocati nell'indovinare le soluzioni di controversie in materia di assicurazioni innanzi al *Financial Ombudsman* [18]. Ancora, più di recente, sono stati sviluppati sistemi per prevedere l'esito di controversie innanzi alla Corte Suprema degli Stati Uniti [19] e la Corte Suprema francese [20].

L'algoritmo predittivo consente, si dice, di arrivare a una forma di giustizia "prevedibile". Una giustizia emessa da un giudice-Robot al riparo di errori e pregiudizi cognitivi. Il sottotesto di queste considerazioni, volendo sintetizzare e usare una massima caricaturale è che la giustizia algoritimica ci consente di superare quella umana legata a *ciò che i giudici mangiano (o non mangiano) a colazione*. Certo se ciò fosse vero, non vi sarebbe dubbio che ricorrere all'IA potrebbe significare assicurare una giustizia migliore. Ma sappiamo che così non è perché l'algoritmo funziona solo all'interno degli schemi in cui è stato programmato, non è in grado di affrontare cambi radicali di paradigma. Cambi di paradigma che nel diritto penale ci sono.

3.3. Compliance *predittiva*

Non mi soffermo oltre sul tema della giustizia predittiva [21], e proseguo spostandomi nel mondo della *compliance* aziendale, concetto, e sto semplificando,

è stato basato su un *dataset* più ampio della precedente ricerca (11,500 casi rispetto ai 584 profilati in precedenza), attraverso cui sono stati valutati un'ampia varietà di modelli neurali. La ricerca è scaricabile da: *https://aclanthology.org/P19-1424.pdf*. Profilo diverso è quello di *Toga*, strumento informatico – ideato da un magistrato bolognese – che si pone l'obiettivo di supportare gli operatori del diritto nei calcoli procedimentali. In questo caso, il *software* non incide sulla fattispecie concreta ma su quella astratta: caricate nel sistema tutte le tipologie di reato previste dal codice e dalla legislazione speciale, il sistema consente di calcolare, ad esempio, il tipo di pena da irrogare, la configurazione di pene accessoria, l'ammissibilità della messa alla prova, la procedibilità e così via.

[18] Come riportato da E. GABELLINI, *La "comodità del giudicare": la decisione robotica*, in *Rivista trimestrale di diritto e procedura civile*, 2019, pp. 1309-10.

[19] D.M. KATZ, M.J. BOMMARITO, J. BLACKMAN, *A General Approach for Predictive the Behavior of the Supreme Court of the United States*, in *PloS ONE*, 2019, consultabile su *https://doi.org/10.1371/journal.pone.0174698*.

[20] O.M. SULEA, M. ZAMPIERI, M. VELA, J. VANGENABITH, *Predicting the Law Area and Decision of the French Supreme Court Cases*, in *arXiv*, 2017, consultabile su: *https://arxiv.org/pdf/1708.01681.pdf*.

[21] Sul punto rinvio agli ampi approfondimenti presenti in letteratura, tra i tanti: F. DONATI, *Impieghi dell'Intelligenza artificiale a servizio della giustizia. Tra rischi e opportunità*, in

in cui possiamo ricomprendere ogni forma di autoregolamentazione in funzione preventiva dell'impresa. La predisposizione di programmi di organizzazione (di processi) aziendale diventa funzionale e preordinata alla previsione e riduzione del rischio della commissione di reati e di illeciti. Volendo sintetizzare (e, ancora una volta, semplificare) al massimo, lo scheletro di ogni meccanismo di *compliance* è costruito intorno ai tre pilastri del «*preventing, detecting and reporting*» con la conseguente necessità di: elaborare procedure di prevenzione in base a rischi specifici e concreti; predisporre organismi o funzioni a presidio delle modalità di prevenzione; originare flussi informativi deputati ad *allarmare* in caso di fatti connessi proprio alla prevenzione dei reati.

È evidente, allora, che le potenzialità della tecnologia in questo settore sono molte.

In quest'ambito, accanto all'uso dell'IA per gestire la complessità viene in aiuto anche le tecnologie di *blockchain*, basate sulle cd. *distributed ledger technologies*. Si tratta di una sorta di registro digitale permanente, distribuito e gestito da una rete nella quale ogni nodo può accedere e conservare, quanto immesso da tutti. I nodi sono dei computer o dei server su cui sono copiate le informazioni relative a tutte le attività registrate nel *libro mastro* (*ledger*). Queste informazioni vengono poi processate da algoritmi che le trasformano in un codice. In tal modo il registro memorizza i dati in gruppi, detti blocchi; ogni blocco, convalidato secondo un protocollo condiviso, è crittografato per legarsi al blocco precedente, formando senza l'intervento di un soggetto terzo (autorità o intermediario) una catena – una catena di blocchi – relativa a dati marcati temporalmente, immodificabili e in continua crescita. La caratteristica di tale tecnologia è la sua natura decentralizzata e distribuita che consente che la manipolazione delle registrazioni possa avvenire solo con la partecipazione di tutti i membri del *network*. Da ciò deriva che il dato inserito e fatto circolare nei sistemi di *blockchain* è controllabile da tutti gli utenti autorizzati senza l'intervento di una autorità terza [22].

Nella prospettiva della *compliance* preventiva si è rilevato come le caratteri-

AI Anthology, cit., p. 179 ss.; O. DI GIOVINE, *Il "judge-bot"*, cit.; M. CATERINI, *Il giudice penale robot*, cit.; E. RULLI, *Giustizia predittiva, intelligenza artificiale e modelli probabilistici. Chi ha paura degli algoritmi?*, in *Analisi giuridica dell'economia*, 2018, p. 533 ss.

[22] Tecnicamente, la *blockchain* è un sistema di registrazione e di archiviazione di dati su cui è possibile raggiungere il consenso in forma decentrata, poiché i blocchi di transazione possono essere solamente aggiunti, ma mai modificati o eliminati, v. S. CAPACCIOLI, *Blockchain*, in G. ZICCARDI, P. PERRI, *Dizionario Legal tech*, Giuffrè Francis Lefebvre, Milano, 2020, p. 120 e bibliografia lì indicata. Sulle *blockchain*, cfr. anche N. ABRIANI, G. SCHNEIDER, *Diritto delle imprese*, cit., p. 30 ss.; M. PALAZZO, Blockchain *e cripo-attività*, in *Il diritto nell'era digitale*, cit., p. 211 ss.

stiche di immodificabilità, decentralizzazione e resilienza siano funzionali alla prevenzione dei reati e, in una fase successiva, allo svolgimento di efficaci investigazioni interne. In ipotesi, si immagina una *blockchain* privata, costituita da nodi coincidenti con realtà interne all'ente (per ipotesi, OdV, collegio sindacale, Responsabile Antiriciclaggio, e così via), governato a livello centrale ma con una gestione decentralizzate delle informazioni, che spetterebbe a ogni *nodo* del registro. In questo modo ciascun nodo (singole funzioni, organi di gestione, ma anche collegio sindacale o OdV) può inserire informazioni e conservare dati. Al tempo stesso, in quanto registro centralizzato, la cancellazione dei dati potrebbe avvenire solo se validata da tutti i nodi. Così, immaginando che l'OdV rappresenti un nodo della *blockchain* nessuna informazione potrebbe essere alterata senza il suo espresso consenso [23].

È chiaro che la diffusione della *blockchain* nel campo societario suscita nuove e importanti questioni sia di sicurezza – questa stessa tecnologia è soggetta a forme di *phishing* – sia sul *come* e *perché* viene utilizzata, con rischi non marginali di manipolazioni e strumentalizzazioni. E quindi, in definitiva, la *blockchain* deve essere controllata e gestita.

L'IA, propriamente detta, quella dell'apprendimento automatico, si pone comunque su un piano diverso dalle stesse tecnologie informatiche più avanzate aiutando gli amministratori a far fronte a realtà imprenditoriali e organizzative sempre più complesse e che si evolvono velocemente, assicurando un punto di vista non *emotivo* e più basato sui fatti.

Poiché allo stato attuale la forza dell'IA sta nella sua capacità di apprendimento attraverso i dati, è in questa accezione che all'interno delle realtà aziendali se ne fa sempre di più uso. In particolare, nelle aziende operano forme di IA assistita o aumentata [24]. Si affidano cioè a dei gestionali informatici o alcuni compiti specifici o gli stessi affiancano le risorse umane in taluni processi

[23] A. GULLO, *I modelli organizzativi*, in G. LATTANZI, P. SEVERINO (a cura di), *Responsabilità da reato degli enti*, vol. I, *Diritto sostanziale*, Giappichelli, Torino, 2020, p. 287.

[24] G. COMANDÉ, *Intelligenza artificiale e responsabilità tra* liability *e* accountability. *Il carattere trasformativo dell'IA e il problema della responsabilità*, in *Analisi giuridica dell'economia*, 2019, p. 169 ss. Nel dettaglio, l'IA può contribuire con intensità modulabile al funzionamento dell'organo amministrativo; in proposito si può distinguere tra: *IA assisted* (di supporto su compiti specifici), *IA augmeted* (di affiancamento e consolidamento dell'organo decisore), *IA amplified* (di co-decisione uomo macchina), di *IA autonomous* (di sostituzione integrale da parte della macchina) e di *IA autopoietic* (di sviluppo autogestito dell'intelligenza artificiale. Su questo, cfr. A. SACCO GINEVRI, *Intelligenza artificiale e* corporate governance, in *Il diritto nell'era digitale*, cit., p. 433; M. LILLÀ MONTAGNANI, *Il ruolo dell'intelligenza nel funzionamento del consiglio di amministrazione delle società per azioni*, Egea, Milano, 2021.

decisionali. Si tratta, allora, di situazioni in cui non vi è una sostituzione con l'essere umano ma un sostegno, un sostegno abile di per sé e non meramente servente [25].

L'utilizzo di *software* gestionali è indispensabile per garantire la conformità normativa dell'operatività aziendale. La costruzione di un adeguato assetto societario può quindi richiedere il ricorso all'IA, che, in una certa misura, può essere paragonata alla necessità di ricorrere alla esternalizzazione di alcune funzioni aziendali. In tali ipotesi, la società che si affida all'intelligenza artificiale deve individuare quali risorse umane e tecnologiche sono in grado di evitare che il *deep learning* li trasformi in *black boxes* ingovernabili [26]. Vanno poi stabilite regole e procedure che assicurino un continuo monitoraggio sull'intelligenza artificiale.

Si è in merito osservato che, nell'ipotesi di costruzione di assetti organizzativi legati alla macchina artificiale, si pone il tema dei possibili riflessi sulla configurabilità della colpa di organizzazione quando il *deficit* organizzativo sia riportabile all'algoritmo [27]. Si aprono, in tal modo, complesse questioni, sovrapponibili a quelle che si agitano sul diverso terreno della ricostruzione delle responsabilità in relazione a eventi legati alla circolazione delle auto a guida automatica [28].

Sul fronte del processamento dei dati si verifica l'impiego più utile della IA, consentendo alla sua capacità di inglobare masse di *big data* di riflettere immedia-

[25] Sull'uso dell'IA quale ausilio alla costruzione degli assetti societari, cfr. A. NUZZO, *Algoritmi e regole*, in *Analisi giuridica dell'economia*, 2019, p. 39 ss.; G.D. MOSCO, *Roboboard. L'intelligenza artificiale nei consigli di amministrazione*, in *Analisi giuridica dell'economia*, 2019, p. 247 ss.; M. CARPENTER, S.H. POON, *Lesson Learned from AI Prototype Designed for Corporate AGM*, 2018, in *https://ssrn.com./abatract=3244160*; N. BURRIDGE, *Artificial Intelligence Gets a Seat in the Boardroom*, in *Nikkei Asian Review*, 2017, *https:// asia.nikkei.com*; S. BAYERN, T. BURRI, D.T. GRANT, M.D. HÄUSERMANN, F. MÖSLEIN, R. WILLIAMS, *Company Law and Autonomous Systems: A Blueprint for Lawyers, Entrepreneurs and Regulators*, in *Hastings Science and Technology Law Journal*, 2, 2017, p. 135 ss.

[26] Come sottolinea G.D. MOSCO, *L'intelligenza artificiale*, cit., talvolta l'autoapprendimento dell'IA rende impossibile riscostruire l'esatta sequenza delle operazioni e delle istruzioni che hanno portato un dato significato. Ricorda l'autore, p. 250, come sia successo «varie volte, come nel famoso caso nel quale due robot, Bob e Alice, hanno iniziato a usare tra loro un nuovo linguaggio incomprensibile ai programmatori, costretti alla fine ad arrendersi e a "staccare la spina". Non a caso, si parla del rischio di "scatole nere"». Su questo anche W. PUGH, *Why not Appoint an Algorithm to Your Corporate Board?, Future Tense*, 2019, in *https://slate.com*.

[27] A. GULLO, *I modelli organizzativi*, cit., p. 284 ss.

[28] Cfr., anche per ulteriori riferimenti bibliografici, F. BARTOLINI, *Auto a guida autonoma e problemi di responsabilità civile*, in *Il diritto nell'era digitale*, cit., p. 299 ss.

tamente *red flags*; potendo procedere al costante monitoraggio di *mail*; predisponendo *report* in tempo quasi immediato agli amministratori – o anche all'OdV [29].

Attraverso l'uso di gestionali a base algoritmica, sul piano della *compliance*, l'ente potrà *ex ante* effettuare diagnosi dei rischi così da essere poi in grado di adottare/rivedere le relative cautele ed *ex post* formulare analisi accurate delle eventuali *non conformità* [30]. A questo si aggiunga poi la capacità di questi algoritmi di fare emergere segnali di allarme anche in ipotesi durante lo svolgimento di una procedura.

È chiaro che per consentire agli algoritmi di analizzare grandi quantità di dati, in modo da poter fare cose che, secondo una nota definizione di qualche anno fa, richiederebbero intelligenza se fatte da persone, è fondamentale l'attività di progettazione e taratura del *software* gestionale del quale ci si avvale. È dal meccanismo di costruzione della "macchina" che dipende la risultanza cognitiva della macchina stessa. È necessario, quindi, istruire il gestionale preposto, proprio perché in questa attività la qualità, la quantità dei dati, il contesto di raccolta e le modalità di selezione sono centrali.

In breve, in caso di uso di algoritmi predittivi nella gestione della *compliance*, occorre mettere a punto una politica che, nell'ambito dei complessivi assetti societari, mantenga il controllo della società sull'AI, tanto nella fase di avvio, quanto mentre questa opera: la società deve essere sempre in grado di accorgersi di eventuali errori degli algoritmi intelligenti e di correggerli rapidamente, presidiandone nel continuo i rischi.

3.3.1. *Il caso dell'antiriciclaggio*

Un esempio dell'uso di dispositivi algoritmici può aversi nella *compliance* antiriciclaggio, dove, come espressamente previsto dal decreto n. 231/2007, i sog-

[29] L'espressione *big data* si riferisce a masse enormi di dati universali per oggetto e soggetto, variabili per capacità auto-generativa, veloci per la formazione *in progress* del patrimonio informativo. In proposito, T. NUMERICO, *Big date e algoritmi*, cit., *passim*. Sulla *querelle* definitoria la dottrina americana (D. LANEY, *3-D data management: controlling data volume, velocity and variety*, 2001, in *https://blogs.gartner.com/doug-laney/files/ 2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf*) si era attestata sulle quattro V, in seguito è ricorsa a una quinta "v", quella del valore, economicamente inestimabile, anche se questa non è una buona ragione per negare loro questo attributo (J. GANTZ, D. REINSEL, *Extracting value form chaos*, in *IDC iView*, 2011, in *http://www.emc.com/collater /analyst-reports/idc-extracting-value-fdrom-chaos-ar.pdf*; B. MARR, *Big data: The 5 V everyone must know*, 2014, in *https://www.linkedin.com/pulse/20140306073407-64875646-big-data-the-5-vs-everyone-must-know*). Sui *big data* e le loro ricadute giuridiche, cfr. G. DE MINICO, Big Data *e la debole resistenza delle categorie giuridiche*. *Privacy e lex mercatoria*, in *Dir. pubbl.*, 2019, p. 89 ss. V. anche bibliografia nella nota 12.

[30] A. GULLO, *I modelli organizzativi*, cit., p. 287.

getti obbligati possono – nel calcolare il rischio di riciclaggio – utilizzare supporti informatici/gestionali. Questi sono, di regola, usati nello svolgimento degli adempimenti di collaborazione passiva (cosiddetta adeguata verifica della clientela) e attiva (segnalazioni delle operazioni sospette). In effetti in questi ambiti, il flusso di informazioni da processare per decidere il livello di rischio di una data operazione legata a un dato cliente è tale da non poter essere analizzato senza un supporto informatico. È evidente che nella creazione dell'ambiente di lavoro del *software* compito fondamentale, per le esigenze di conformità normativa, è quello di impostare attentamente il "peso" attribuito a ciascun parametro/tab di cui il gestionale sarà composto. E ciò sia per la rilevanza diretta del singolo dato (soppesato in virtù del suo significato, così quanto pesa in termini di rischio un certo luogo geografico) e, in secondo luogo, nell'ottica di (futura) combinazione tra parametri. Errori valutativi in sede di "taratura" e di attribuzione dei "pesi" possono ripercuotersi irreparabilmente sull'*output* che verrà generato dal gestionale. In breve: il *software*, una volta calibrato, sarà in grado di esplicare la propria intelligenza artificiale, ma non mediante un meccanismo di ragionamento autonomo o di conoscenza innata, bensì sulla base di un apprendimento "costruito"; se la costruzione presenta falle o errori di progettazione, il risultato (*output*) sarà inficiato.

Sotto il profilo statico di adempimento degli obblighi di collaborazione passiva (adeguata verifica) i problemi inerenti all'intelligenza artificiale si sostanziano nel riuscire a insegnare, al *software*, cosa prendere in considerazione, qual è l'ordine di importanza dei dati, cosa fare alla luce delle varie combinazioni, cosa dire al termine dell'analisi quantitativa e come trasformare un dato informativo in un dato valutativo. Errori in fase di "insegnamento" potrebbero portare a eventuali mancate adeguate verifiche.

Infine, anche in questo caso, il risultato finale, l'*output* prodotto dalla macchina, in base ai principi regolanti la materia quali quelli dell'approccio concreto basato sul rischio e di proporzionalità, deve potere essere oggetto di valutazione, di bilanciamento *umano* che possa anche individuare tra le tante informazioni e dati quali sono gli elementi che generano falsi positivi o errori.

In breve, in caso di uso di algoritmi predittivi nella gestione della compliance, occorre mettere a punto una politica che, nell'ambito dei complessivi assetti societari, mantenga il controllo della società sull'AI tanto nella fase di avvio, quanto mentre questa opera: la società essere deve sempre in grado di accorgersi di eventuali errori degli algoritmi intelligenti e di correggerli rapidamente, presidiandone nel continuo i rischi.

3.4. *Per concludere*

In definitiva, l'essere umano, la persona con i suoi pregiudizi, con le sue emozioni, con la sua flessibilità e capacità di adattare anche il processo decisionale alle circostanze del caso rimane centrale.

Niente di nuovo, ancora. Già Vico ci ricorda come la matematica, al pari della storia, sia una delle discipline "fatte" dall'uomo, rientrante cioè nel suo dominio conoscitivo [31]. Pertanto, viene da dire oggi, rileggendo Vico: poiché la matematica rientra nel dominio conoscitivo dell'uomo, anche tutte le operazioni matematiche che l'algoritmo è in grado di realizzare a una straordinaria velocità vi rientrano. A ben vedere, poi, ciò che inquieta nel calcolo algoritmico e la sua velocità. Tuttavia, come ci ricorderebbe Vico, anche quelle algoritmiche in quanto operazioni matematiche sono programmate dall'uomo e, pertanto conoscibili, controllabili, modificabili [32].

E ciò che rileva nel continuo gioco tra la nostra intelligenza e quella artificiale è proprio la capacità di gestire il controllo delle operazioni.

Non mi sfugge che le mie, poche, riflessioni siano un tentativo per scrollarmi di dosso regressioni tecnofobiche, pregiudizi antimacchinici. La sfida che le nuove tecnologie ci impongono ci impone un *nuovo stile di pensiero.*

Tuttavia, non possiamo dimenticare che ogni processo decisionale, e quindi anche il rendere giustizia nel cui esercizio gli esseri umani sono avvantaggiati rispetto alle macchine per la loro maggiore sensibilità che li porta a saper cogliere molteplici sfumature [33] è legato a stati emozionali. La giustizia è, lo si è già detto [34], una esperienza profondamente umana, legata quindi alle emozioni: *fare giustizia* è enormemente più complesso di *applicare la legge* [35]. Ponendomi in un solco tracciato da altri [36], mi sembra che si possa dire che le emozioni giocano

[31] A. PUNZI, *Il diritto e i nuovi orizzonti dell'intelligenza umana*, in *Analisi giuridica dell'economia*, 2019, p. 25.

[32] A. PUNZI, *Il diritto e i nuovi orizzonti*, cit., p. 26.

[33] Così, O. DI GIOVINE, *Il "judge-bot"*, cit., p. 965.

[34] Mi sia consentito rinviare al mio, *Le emozioni del giudice (penale)*, in *Archivio penale*, 3, 2021.

[35] Così, C.V. GIABARDO, *Il giudice e l'algoritmo (in difesa dell'umanità del giudicare)*, cit.

[36] Mi riferisco, in particolare, alla filosofa Martha Nussbuam, voce tra le più autorevoli nell'indicare la centralità della dimensione umana o emotiva del diritto, di cui, tra gli altri, M. NUSSBUAM, *L'intelligenza delle emozioni*, Il Mulino, Bologna, 2004, e *Emozioni politiche*. *Perché l'amore conta per la giustizia*, Il Mulino, Bologna, 2013. Nella letteratura penalistica, il riferimento è a O. Di Giovine, di cui, tra gli altri, *Una lettura evoluzionistica del diritto penale. A proposito delle emozioni*, in O. DI GIOVINE (a cura di), *Diritto penale e neuroetica*, Cedam, Padova, 2013, e *Un diritto penale empatico? Diritto penale, bioetica e neuroetica*, Giappichelli, Torino, 2009.

un ruolo importante nel processo di formazione della decisione giudiziaria insieme a una definizione completa e "ragionevole" dei casi stessi. È necessario riconoscere, come detto, anche alle emozioni una valenza cognitiva, avendo anche loro a che fare con il pensiero e con il ragionamento in qualsiasi forma. Le stesse non possono essere criminalizzate come sicuri fattori di distorsione della razionalità al contrario consentendoci di pesare, ai fini decisionali anche i valori.

Concludo, ricordando quello che l'IA ancora non possiede; le sue *mancanze* che, al momento, ci impediscono di utilizzarla come sostituto dell'uomo.

L'IA non ha ancora capacità intuitiva, non ha intelligenza emotiva, empatia, etica, fantasia; «non è in grado di combinare visione e passione, combinazione necessaria per elaborare strategie e assumere decisioni anche per gli altri; non ha piena consapevolezza di sé e delle conseguenze dei suoi comportamenti e delle sue scelte» [37]. Trattandosi di *matematica*, direbbe Vico, non deve occuparsi del senso di ciò che compie. La scienza, infatti, non ha il compito di spiegare qual è il significato delle forze che tengono legati gli atomi gli uni agli altri.

Ciò che in definitiva manca all'algoritmo è una vera e propria identità.

In attesa della costruzione di questa identità, temo, allora, che ci tocchi continuare ad avere a che fare con noi umani, sempre più umanoidi che, forse, dipendiamo anche da ciò che abbiamo mangiato o non mangiato a colazione.

E di questo, certo, mi dolgo.

[37] G.D. MOSCO, *L'intelligenza artificiale*, cit., p. 251.

CAPITOLO IV

L'implementazione delle nuove tecnologie nelle politiche anticorruzione

FEDERICA DE SIMONE

SOMMARIO: 4.1. Prolegomeni del rapporto tra lo sviluppo tecnologico e l'ordinamento giuridico. – 4.2. Alcune ipotesi classificatorie. – 4.3. Aspetti problematici. – 4.4. Corruzione e intelligenza artificiale, un efficace connubio? – 4.4.1 Il sistema cinese *Zero Trust*. – 4.4.2 L'esperienza spagnola: le cd. *mappe autorganizzanti*. – 4.5. Lo strumento della *blockchain*. – 4.6. Il difficile contemperamento tra tutela e progresso. – 4.7. Riepilogando.

4.1. *Prolegomeni del rapporto tra lo sviluppo tecnologico e l'ordinamento giuridico*

Per introdurre il tema del rapporto tra le nuove tecnologie e il diritto penale, sono indispensabili due premesse di fondo [1].

La prima considerazione ha carattere generale e riguarda il progresso tecnologico e la velocità con cui i nuovi strumenti invadono la nostra vita in maniera alcune volte anche inconsapevole. È sotto gli occhi di tutti che l'umanità sta attraversando il periodo a più alto tasso di innovazione mai visto sin ora, in cui scenari inimmaginabili solo fino a poco tempo fa si stanno concretizzando, offrendo notevoli opportunità.

La concezione marxista del progresso considera quest'ultimo la regola, di

[1] Il tema sembra essere di assoluta novità, tuttavia i tentavi di implementare il calcolo computazionale nelle decisioni giudiziali risale addirittura a Leibniz. Cfr. P. MORO, C. SARRA, *Tecnodiritto. Temi e problemi di informatica e robotica giuridica*, Milano, 2017, p. 32. Per un inquadramento generale, si veda L. PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Cybercrime*, Milano, 2019, p. 35 ss.

natura tecnologica, posta a fondamento dell'evoluzione [2], con la conseguenza che qualsiasi tentativo di bloccare o anche solo ritardare lo sviluppo sarebbe impossibile se non vano. D'altronde, la storia ci ha insegnato che spesso scenari apocalittici paventati a seguito dell'introduzione di nuove scoperte scientifiche sono, poi, svaniti, lasciando il posto a cambiamenti epocali positivi. È stato così per la scrittura, osteggiata dai filosofi greci in quanto considerata la causa della perdita della capacità di ricordare a memoria, di raccontare e anche di usare la fantasia. Lo stesso è avvenuto con l'avvento della stampa, che – secondo i suoi detrattori – rendendo alla portata di tutti il sapere e la conoscenza avrebbe determinato una grave crisi nell'umanità, e della televisione, accusata di incidere in negativo sulla capacità dell'uomo di socializzare con i suoi simili [3].

Un'intelligenza artificiale che possa avere un ruolo nel migliorare i tempi della giustizia, piuttosto che un sistema di reti neurali da impiegare nel contrasto al fenomeno della corruzione sono solo da salutare con favore anche se con le opportune cautele.

La seconda premessa è di tipo tecnico e concerne la necessità – ormai non più rinviabile – di un intervento regolativo, che disciplini l'impiego delle nuove tecnologie alla luce dei principi ordinamentali. Si tratta di una esigenza avvertita da più parti e che emerge preponderante anche dai numerosi documenti prodotti sia a livello sovranazionale sia nazionale, a cominciare dalla Carta etica sull'intelligenza artificiale [4] del 2018 e al Libro bianco [5] della Commissione europea del 2020, sino al documento presentato dal Parlamento e dal Consiglio europeo nel 2021 come Proposta di Regolamento sull'approccio europeo per l'intelligenza artificiale [6].

L'Unione europea ritiene, infatti, che i pericoli connessi all'uso massivo di queste tecnologie, indipendentemente dal loro campo di applicazione, possano essere troppo elevati, soprattutto rispetto alle esigenze di tutela dei diritti umani. Più evidenti sono i rischi riguardanti la violazione della vita privata, dei dati personali e del divieto di discriminazione, oltre a quelli relativi all'accesso alla giu-

[2] Così K. MARX, *Das Kapital*, 3 voll., Hamburg, 1867-1894 (tr. it. a cura di A. MACCHIORO, B. MAFFI, *Il capitale*, Milano, 2017, 3).

[3] Cfr. W. SCHMITZ, *Oltre Benjamin. "La riproducibilità tecnica della scrittura" e la diffidenza verso la stampa tipografica nell'Europa del Quattrocento*, in TECA, Univ. di Bologna, 2021, 11, p. 7 ss.

[4] Cfr. *https://rm.coe.int/carta-etica-europea-sull-utilizzo-dell-intelligenza-artificiale-nei-si/1680993348*.

[5] In *https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_it.pdf*.

[6] Si veda *https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0006.02/DOC_1&format=PDF*.

stizia; tuttavia, l'elenco è solo esemplificativo e molti altri possono essere i diritti lesi o posti in pericolo [7].

Sul piano internazionale la posizione europea non è pacificamente condivisa. Diametralmente opposta – ad esempio – quella americana, che predilige un approccio liberale alla stessa stregua del *free marketplace of ideas* di miltoniana memoria [8]. Un simile orientamento potrebbe, tutt'al più, essere condivisibile in astratto se posto a fondamento della sola libertà di stampa. La garanzia piena e non condizionata del diritto alla libera manifestazione del pensiero in ogni sua forma potrebbe determinare, infatti, l'affermazione della verità alla stessa stregua di quanto avviene nel libero mercato delle merci. Purtuttavia, sembra alquanto inappropriata l'applicazione concreta del principio della concorrenza alla circolazione delle idee che, infatti, incontra un primo limite in riferimento al problema delle *fake news* [9].

Attualmente, la diffusione di notizie false tramite *internet* è incontrollata e in alcun modo circoscrivibile e diversi studi hanno sottolineato i rischi che ne possono derivare in termini di tenuta dei sistemi democratici, tanto da invocare anche in questo caso un intervento normativo su più livelli [10].

A maggior ragione, la linea dettata dalla concezione americana appare ancor meno condivisibile se applicata anche all'impiego di nuove tecnologie come intelligenza artificiale, algoritmi e reti neurali. In tal caso, lasciare che sia il libero

[7] Così *https://fra.europa.eu/sites/default/files/fra_uploads/fra-2021-artificial-intelligence-summary_it.pdf*.

[8] La metafora del libero mercato applicato alle idee si deve a JOHN MILTON, che nel 1644 scrisse il saggio *Areopagitica*. Per la versione in italiano, si veda M. GATTI, H. GATTI (a cura di), *Discorso per la libertà di stampa*, Milano, 2002. Per una ricostruzione della teoria del *marketplace of ideas*, si veda *ex multis* G. PITRUZZELLA, O. POLLICINO, S. QUINTARELLI, *Parole e potere. Libertà di espressione*, *hate speech*, *fake news*, Milano, 2017.

[9] Sul tema si veda T. GUERINI, *Fake news e diritto penale*, Torino, 2020.

[10] In ambito europeo, l'ultimo provvedimento rilevante in materia è la Proposta di Regolamento del parlamento europeo e del consiglio sul mercato unico dei servizi digitali (legge sui servizi digitali) e modifica della direttiva 2000/31/CE del 15 dicembre 2020, su cui è stato trovato un accordo il 23 aprile 2022. Purtroppo, il provvedimento è stato bocciato dallo stesso Parlamento il 13 giugno 2022 in quanto il testo è stato ritenuto non conforme a quanto previsto dall'accordo. Cionondimeno, costituisce un riferimento normativo importante a cui guardare e che, con ogni probabilità, vedrà comunque la luce una volta trovata l'intesa. Cfr. *https://ec.europa.eu/info/sites/default/files/proposal_for_a_regulation_on_a_single_market_for_digital_services.pdf* e *https://www.cybersecurity360.it/legal/il-parlamento-ue-boccia-il-testo-del-digital-services-act-ecco-cosa-puo-succedere-ora/*. In Italia, il dibattito parlamentare ha dato luogo ad alcune proposte legislative, che non hanno – però – trovato un seguito. Sia consentito un rinvio a F. DE SIMONE, *"Fake news", "post truth", "hate speech": nuovi fenomeni sociali alla prova del diritto penale*, in *Arch. pen*., 2018, 1, pp. 1-49.

mercato a far prevalere una tecnica anziché un'altra, non si comprende in che modo potrebbe risolvere – ad esempio – il problema dei pregiudizi, né tanto meno della cosiddetta *black box*. Invero, piuttosto che rispondere a logiche di garanzie e tutele, un simile approccio sembra celare la prevalenza di scopi ben meno nobili, correlati a esigenze di natura prevalentemente commerciale e consumistica. Basti pensare alle politiche di colossi come *Facebook* o *Amazon*, che negli USA impiegano algoritmi discriminatori o di tracciamento che in Europa non sarebbero consentiti proprio grazie alla regolamentazione di *soft law* e alla normativa già vigente.

In ultimo, l'approccio cinese non si preoccupa di dissimulare gli obiettivi di pieno controllo sociale e in maniera esplicita intende sfruttare proprio tutti gli aspetti che per noi europei sono critici per i diritti fondamentali, per assicurare il mantenimento dello *status quo*.

Inarrestabilità del progresso e contestuale irrinunciabilità della regolamentazione sembrano premesse indispensabili rispetto alla necessità di riconoscere un ruolo centrale al diritto, chiamato – come sempre avviene nei momenti di cambiamento epocale – a svolgere la funzione immunizzante e di stabilizzatore sociale teorizzata da Luhmann [11]. Ciò assume una rilevanza pregnante nello specifico dell'impiego dei sistemi di intelligenza artificiale, i quali si trovano a ricoprire ruoli anche molto diversi tra loro all'interno della società [12], con implicazioni sia di natura giuridica, sia di carattere etico [13].

4.2. *Alcune ipotesi classificatorie*

L'individuazione di alcune ipotesi classificatorie in cui far rientrare le nuove tecnologie può risultare utile ai fini di un inquadramento del tema nell'ambito giuridico, con particolare riguardo alla materia penale.

Una prima classificazione potrebbe portare a distinguere i nuovi strumenti in base al ruolo di soggetto attivo o passivo dell'illecito penale, a seconda se assumano la veste ora di autore ora di vittima del reato.

[11] Così N. LUHMANN, *Ausdifferenzierung des Rechts: Beiträge zur Rechtssoziologie und Rechtstheorie*, Frankfurt, 1981, in R. DE GIORGI (trad. it a cura di), *La differenziazione del diritto: contributi alla sociologia e alla teoria del diritto*, Bologna, 1990, pp. 1-397.

[12] Si veda F. BASILE, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *https://dirittopenaleuomo.org/contributi_dpu/intelligenza-artificiale-e-diritto-penale-quattro-possibili-percorsi-di-indagine/*, 29 settembre 2019; ID., *Intelligenza artificiale e diritto penale: qualche aggiornamento e qualche nuova riflessione*, in questo Volume, pp. 1-17.

[13] Cfr. G. TAMBURRINI, *Etica delle macchine. Dilemmi morali per robotica e intelligenza artificiale*, Roma, 2020; P. BENANTI, *Oracoli. Tra algoretica e algocrazia*, Roma, 2018.

Le ipotesi in cui l'intelligenza artificiale si comporta alla stregua di un reo costituiscono una casistica abbastanza nota e ampia, ma non per questo scevra di criticità. Innanzitutto, vanno distinti i casi in cui il sistema è stato creato allo scopo di porre in essere fatti di reato e i casi in cui, invece, il fatto penalmente rilevante scaturisce da un errore della macchina stessa. Esempi non esaustivi della prima ipotesi sono i *software* ideati per diffondere informazioni false e/o ledere la reputazione altrui, i sistemi finalizzati alla distruzione di altre strutture informatiche, le armi autonome quando pongono in essere condotte rilevanti ai sensi dei codici penali militari in tempo di guerra. Diversamente, appartengono alla seconda ipotesi tutti i casi in cui le nuove tecnologie, pur operando all'interno di un quadro di legalità, determinano delle lesioni a beni giuridici tutelati, inquadrabili nel paradigma colposo.

Nell'ambito della *cybersecurity* si inseriscono la maggior parte dei casi in cui i nuovi sistemi possono essere considerati vittima di reato, in quanto oggetto di attacchi informatici che determinano perdita di dati, alterazione e finanche distruzione dei sistemi [14].

Invero, l'uso dei termini reo e vittima in capo all'intelligenza artificiale non può essere riferito nell'accezione tecnica, non essendo ancora riconosciuta alcuna forma di personalità giuridica che potrebbe giustificare un simile *status* [15]. *De iure condito*, il ruolo in entrambi i casi dovrebbe essere assunto da colui che ha la titolarità del sistema e anche così la sua individuazione non è di pronta soluzione, essendo molteplici gli attori coinvolti [16]. Sarebbe, dunque, più appropriato considerare i nuovi sistemi alla stregua di uno strumento ovvero di un oggetto materiale del reato, almeno sino a quando non si affronterà giuridicamente la questione connessa al riconoscimento della cd. personalità elettronica [17]. L'in-

[14] Gli attacchi *Denial of service* costituiscono lo strumento maggiormente impiegato per danneggiare i sistemi informatici in generale e in tali ipotesi sono rinvenibili una pluralità di vittime. Non solo l'intelligenza artificiale, infatti, può essere danneggiata ma la perdita di dati, ad esempio, può determinare una violazione della *privacy*. Sia permesso un rinvio a F. DE SIMONE, *La rilevanza dei delitti contro l'integrità dei dati dei programmi e dei sistemi informatici al tempo della guerra russo-ucraina*, in *Giur. pen. web*, 2022, 7-8, pp. 1-25.

[15] Cfr. S. RIONDATO, *Robot: talune implicazioni di diritto penale*, in P. MORO, C. SARRA (a cura di), *Tecnodiritto*, cit., p. 85 ss.

[16] I soggetti che sono coinvolti dall'operato dell'intelligenza artificiale sono il proprietario del sistema, il gestore e il suo programmatore. Si discute su quale di questi far ricadere la responsabilità giuridica e in che misura. Sul punto si veda C. PIERGALLINI, *Intelligenza artificiale: da "mezzo" ad "autore" del reato?*, in *Riv. it. dir. proc. pen*., 2020, 4, p. 1745 ss.

[17] Nella Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL),

troduzione di un *tertium genus* accanto alla responsabilità fisica e giuridica potrebbe avere ricadute molte ampie e imporre un ripensamento del sistema soprattutto in riferimento al tema della funzione della pena e al catalogo delle sanzioni da irrogare.

Una seconda ipotesi classificatoria si potrebbe individuare tenendo conto delle funzioni svolte dall'intelligenza artificiale nel momento di prevenzione del crimine e in quello di accertamento in fase processuale. In particolare, ci si riferisce ai casi in cui i nuovi sistemi sono utilizzati alla stessa stregua di un consulente tecnico. Si tratta di un ruolo che può essere svolto al servizio della polizia giudiziaria per quanto concerne le attività di predizione, prevenzione e scoperta del crimine, ovvero in ausilio al giudice per valutare la pericolosità sociale di un soggetto o anche per decidere le sorti di un caso [18]. Strumenti come *XLaw*, in uso alla questura di Napoli per la prevenzione dei crimini, o sistemi algoritmici come *Compass* in USA e *Hart* in Inghilterra impiegati nella valutazione del rischio di recidiva ai fini della concessione di una misura alternativa sono già da tempo in dotazione alla polizia o al giudice con risultati soddisfacenti, sebbene le criticità rilevate – di cui si dirà più avanti – non siano poche.

La figura del consulente algoritmico in ambito giudiziario dovrebbe suscitare minori perplessità rispetto ai casi in cui l'intelligenza artificiale sia impiegata in funzione predittiva. I codici di rito, infatti, già prevedono che un tecnico coadiuvi il giudice nella sua attività e in tale caso specifico il consulente metterebbe al servizio della giustizia una quantità di dati molto maggiori rispetto al consulente umano. Ciò che invece fa vacillare le certezze dei giuristi è l'attività predittiva, eppure, con le probabilità e le percentuali – soprattutto i penalisti – dovrebbero essere avvezzi, costituendo la regola quando si tratta di stabilire il nesso causale tra un evento e una condotta.

alla lett. f) dell'art. 59 si legge che va valutato l'impatto «*dell'istituzione di uno* status *giuridico specifico per i* robot *nel lungo termine, di modo che almeno i robot autonomi più sofisticati possano essere considerati come persone elettroniche responsabili di risarcire qualsiasi danno da loro causato, nonché eventualmente il riconoscimento della personalità elettronica dei robot che prendono decisioni autonome o che interagiscono in modo indipendente con terzi*». Cfr. *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52017IP0051*. L'ambito è quello della responsabilità civile e ha sollevato molte critiche e opinioni discordanti, ma la possibilità di introdurre un *tertium genus* di personalità che abbia delle implicazioni anche penalistiche è già oggetto di approfondimenti in dottrina. Si veda G. HALLEVY, *The Basic Models of Criminal Liability of AI Systems and Outer Circles*, 2019, in *http://dx.doi.org/10.210139/ssrn.3402527*; U. RUFFOLO, *Il problema della personalità elettronica*, in *Journal of Ethics and Legal Technologies*, 2020, 2(1), p. 75 ss.

[18] V. MANES, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in U. RUFFOLO (a cura di), *Intelligenza Artificiale. Il diritto, i diritti, l'etica*, Milano, 2020, p. 547 ss.

Invero, in tema di predittività è necessario distinguere tra predizione, prevedibilità e probabilità, anche perché il termine *predictive* in italiano non ha un corrispondente significato univoco e il comune sentire riporta l'idea di predire un determinato evento come se si trattasse di indovinare il futuro alla stessa maniera di un oracolo [19]. Dal canto suo la nozione di probabilità rinvia a un'inferenza statistica ossia alla deduzione di un risultato da una percentuale indicata che seppure sotto la coperta della scienza non significa certezza, semmai restituisce proprio un'idea di incertezza, idea distopica, a sua volta, rispetto alla prevedibilità, che invece richiama in un certo qual modo la certezza.

Sembra uno scioglilingua ma non lo è perché – come accennato prima – si tratta di concetti particolarmente cari ai penalisti. La probabilità è alla base della ricostruzione del nesso causale [20] che lega l'evento alla condotta del soggetto agente, la prevedibilità fonda il principio di legalità all'art. 25, comma 2, Cost. ma lo ritroviamo ad esempio anche nella valutazione dell'elemento soggettivo, mentre la predittività sembra collocarsi nell'ambito della valutazione del rischio – per esempio – da recidiva. D'altronde, la valutazione della pericolosità e anche il cd. *risck assestment* sono concetti nati a inizio '900 con la scienza criminologica e quando un giudice opera una valutazione sulla pericolosità di un reo in merito all'ammissione a una misura alternativa nessuno si chiede se sta prevedendo il futuro o applicando una probabilità statistica [21].

L'intelligenza artificiale, tramite il procedimento di apprendimento automatico di cui si alimenta, rappresenta una sintesi di tutte queste caratteristiche e ciò non deve ingenerare allarme *ex se*, trattandosi di procedimenti analoghi a quelli elaborati dall'uomo, con la differenza che le nuove tecnologie raggiungono migliori risultati rispetto ai fini per i quali sono programmate. Questo è possibile solo grazie all'enorme quantità di dati in più che l'intelligenza artificiale è capace di processare in confronto alla mente umana, null'altro [22].

[19] V. R. BERK, *Machine learning risk. Assessment in Criminal Justice settings*, Svizzera, 2019, *passim*.

[20] In dottrina si sostiene che modelli causali – come anche la sussunzione sotto leggi scientifiche di copertura – possono essere combinati con modelli di previsione, sempre che queste siano accurate e interpretabili. Così R. BERK, *Machine*, cit., p. 155 ss.

[21] La valutazione del rischio criminale in termini di comportamento antisociale è fondata sulla probabilità e sull'individuazione di fattori di rischio. Cfr. S. QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*, Svizzera, 2020, p. 147 ss.

[22] B. OCCHIUZZI, *Algoritmi predittivi: alcune premesse metodologiche*, in *Dir. pen. cont*., 2019, 2, p. 393 ss.

4.3. *Aspetti problematici*

Prima ancora di circoscrivere l'ambito di rilevanza della questione rispetto ai temi propri del diritto penale, è necessario spendere una riflessione in relazione ai problemi posti dall'introduzione delle nuove tecnologie e che non sembrano di facile soluzione, a partire dalla questione definitoria.

Machine learning e *deep learning*, intelligenza artificiale debole e forte, reti neurali, algoritmi, *chatbot*, *blockchain* non sono termini da usare alternativamente come sinonimi ma indicano tecnologie differenti e con proprie peculiarità, a cui destinare in parte regolamentazioni diverse.

Allo stesso tempo, è probabilmente errata la pretesa di imbrigliare le nuove tecnologie in definizioni tecniche precise, vista anche la velocità con cui esse si aggiornano e che costringerebbero ad un continuo adeguamento della normativa. La difficoltà di introdurre definizioni puntuali in tale ambito è al momento tale, che persino il Parlamento europeo sconsiglia una simile operazione [23], soprattutto per evitare il rischio di norme non al passo con la velocità di aggiornamento delle tecnologie.

Così posta la questione definitoria, emerge una contraddizione che non sembra superabile, nella misura in cui la scelta di non adottare definizioni flessibili risponde alle esigenze di aggiornamento in tempo reale dei nuovi sistemi, ma non può collimare con il rispetto di alcuni principi, *in primis* quello di tassatività e determinatezza. Questo sarebbe soddisfatto se il legislatore adottasse una tecnica normativa che proceda per casi e ipotesi; tuttavia, tale scelta presenterebbe non poche difficoltà, a cominciare dal rischio di superfetazione normativa.

Grande peso, poi, va dato ai problemi posti dalla cosiddetta *black box*, alla tutela dei dati utilizzati per l'apprendimento automatico e alla loro qualità, tutti temi per i quali il diritto, pur prevedendo una disciplina specifica, non sembra offrire soluzioni efficaci [24].

Un esempio evidente di quanto appena detto è costituito dal quarto principio della Carta etica [25], che nell'introdurre la trasparenza tecnica e la conoscibilità,

[23] Proprio in quest'ottica, nella Proposta di Risoluzione sulla robotica del 2015 il Parlamento europeo promuove la ricerca di una nozione comune ma al tempo stesso flessibile. Cfr. *https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_IT.html#_section1*.

[24] Si veda C. CASONATO, *IA e giustizia: potenzialità e rischi*, in *DPCE Online*, 2020, in *http://www.dpceonline.it/index.php/dpceonline/article/view/1082*.; B. OCCHIUZZI, *Algoritmi*, cit., p. 393 ss.

[25] Cfr. Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi adottata dalla CEPEJ nel corso della sua 31ª Riunione plenaria (Strasburgo, 3-4 dicembre 2018), in *https://rm.coe.int/carta-etica-europea-sull-utilizzo-dell-intelligenza-artificiale-nei-si/1680993348*.

fa riferimento alla possibilità di ricostruire il percorso decisionale della macchina. Invero, si tratta di un principio di difficile attuazione, nella misura in cui il sistema di autoapprendimento, per la sua stessa strutturazione, esclude una simile possibilità. La pretesa giuridica, infatti, non può essere soddisfatta finanche dal programmatore della macchina, che mantiene il controllo esclusivamente sul pacchetto di dati iniziali con cui ha avviato il procedimento di apprendimento [26].

La complessità della questione emerge, prima ancora di costituire un problema giuridico, a livello di validazione scientifica: se un metodo non può essere provato allora il risultato non è validabile. È il dogma della riproducibilità di Galilei [27] che ben può essere esteso al di fuori dei confini strettamente scientifici, basti pensare alle ricadute che tali sistemi possono avere se impiegati per fondare il quadro accusatorio nel processo penale. *Quid iuris*, quando indicata una prova non si riesce a ricostruire il percorso che ha portato ad essa a causa proprio del problema della *black box*? La questione è emersa, ad esempio, in riferimento all'algoritmo *Zero Trust*, impiegato per la prevenzione e il perseguimento della corruzione in Cina e di cui si dirà più avanti.

L'impossibilità di una validazione scientifica emerge anche tra le righe del settimo dei 23 principi di *Asilomar* [28] stilati nel 2017 e alla cui redazione hanno partecipato tra i più influenti scienziati. La disposizione afferma che se un sistema di intelligenza artificiale causa dei danni, *dovrebbe* essere possibile accertarne il motivo e l'uso del verbo al condizionale lascia pensare sulla reale possibilità di una sua attuazione.

Per quanto concerne il problema dei dati e della loro qualità, mentre nella collettività permane la convinzione che l'intelligenza artificiale sia più obiettiva dell'uomo e come tale preferibile [29], tra gli addetti ai lavori il mito della neutralità delle macchine è già caduto. È, ormai, questione nota che i nuovi strumenti soffrono – come gli uomini – i cosiddetti *bias*, cioè i pregiudizi che condizionano il pensiero dei programmatori e che, inesorabilmente, si riversano nei dati immessi nei sistemi. La questione sarebbe addirittura amplificata nel caso dell'intelligenza artificiale, poiché il sistema apprende ed evolve proprio grazie al pacchetto di dati iniziali immessi dal programmatore per avviare il *machine learn-*

[26] M. ANNANY, K. CRAWFORD, *Seeing without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability*, in *New Media and Society*, 2018, 20, 3, p. 973 ss.

[27] V. G. GALILEI, *Le idee filosofiche, il metodo scientifico*, in S.V. ROVIGHI (a cura di), *Antologia*, Brescia, 2021, pp. 1-208.

[28] Si veda *https://futureoflife.org/2017/08/11/ai-principles/*.

[29] A. GARAPON, J. LASSEGUE, *La giustizia digitale. Determinismo tecnologico e libertà*, Bologna, 2021, p. 241 ss., sottolineano i rischi del mito della delega alle macchine.

ing, con la conseguenza che i pregiudizi alimentano non solo il momento iniziale, ma tutto il procedimento di apprendimento.

La casistica del rischio di lesioni di diritti fondamentali e beni giuridici a causa dei *bias* è sempre più ampia, tra gli esempi l'algoritmo di *Amazon* che per un periodo ha preferito nel reclutamento gli uomini alle donne poiché i dati utilizzati per il *machine learning* erano basati sulle assunzioni di personale maschile degli anni precedenti, o ancora il sistema *Frank* di *Deliveroo* che discriminava i *riders* in base alla *performance*. Ci sono, poi, tutti quei casi in cui siamo del tutto inconsapevoli dell'uso di dati viziati dai pregiudizi, come ad esempio avviene nelle pratiche di concessione dei mutui, condizionate molto spesso da dati quali il codice di avviamento postale.

Il tema dei dati, dunque, è di primaria importanza. Da un lato, se non ci fossero *big data* e *open data* ad alimentare le nuove tecnologie, verrebbe meno la loro stessa potenzialità, dall'altro assicurare la qualità dei dati è essenziale per evitare che l'errore di sistema diventi esso stesso il sistema [30].

4.4. *Corruzione e intelligenza artificiale, un efficace connubio?*

A fronte degli aspetti problematici sin qui segnalati, emergono le positività dell'impiego dei nuovi strumenti, in particolar modo nella prevenzione e nel contrasto dei fenomeni criminosi connessi ai reati predatori e a quelli seriali, per i quali le probabilità di risultati positivi sono risultate piuttosto elevate [31]. È di recente acquisizione, invece, l'uso di reti neurali e sistemi di intelligenza artificiale nel contrasto ai delitti di corruzione.

Il tema è di grande interesse, dal momento che il costo annuale della corruzione nel mondo è stimato in 1 trilione di dollari [32] e solo nell'Unione europea vale 5 bilioni di euro l'anno.

[30] V. C. BURCHARD, *L'intelligenza artificiale come fine del Diritto penale? Sulla trasformazione algoritmica della società*, in *Riv. it. dir. proc. pen*., 2019, 62, 4, p. 1909 ss.

[31] Risultati empirici sono rinvenibili, ad esempio, nelle valutazioni di funzionamento di sistemi come XLaw in uso alla Questura di Napoli. Si veda E. LOMBARDO, *Sicurezza 4P: lo studio alla base del software XLAW per la previsione e la prevenzione dei crimini*, Venezia, 2018, pp. 1-190. Si veda anche R. PELLICCIA, *Polizia predittiva: il futuro della prevenzione criminale?*, in *https://www.cyberlaws.it/2019/polizia-predittiva-il-futuro-della-prevenzione-criminale/*, 9 maggio 2019; G. DI GENNARO, E. LOMBARDO, G. RICCIO, U. RUFFOLO, A.F. URICCHIO, *Intelligenza artificiale e politiche di sicurezza urbana: verso quali modelli?*, Bari, 2020.

[32] Si veda il *Report* del Fondo monetario internazionale, *Fiscal Monitor. Curbing Corrupting*, 2019, in *https://www.anticorruzione.it/portal/rest/jcr/repository/collaboration/Digital%20Assets/anacdocs/Attivita/AttivitaInternazionale/InternationalMonetaryFund.apr.2019.pdf.*

Utilizzando una distinzione mutuata dai paesi di *common law*, il valore della corruzione indicato dal Fondo monetario internazionale include sia la cosiddetta *petty corruption*, sia la *grand corruption*. La distinzione fa riferimento alle due forme più diffuse di corruzione, ossia il pagamento di una tangente da parte di un privato al pubblico ufficiale per l'ottenimento di un servizio dovuto e l'uso improprio di alte cariche e prassi istituzionali finalizzate al conseguimento di benefici individuali o di un ristretto gruppo sociale.

Proprio per questo l'Unione europea considera la lotta alla corruzione un pilastro fondamentale per sostenere lo stato di diritto e, infatti, ha svolto un ruolo importante nell'adozione della Risoluzione sulla lotta alla corruzione adottata dall'Assemblea generale delle Nazioni Unite nel giugno 2020, da cui poi è scaturita la Sessione speciale dell'Assemblea generale delle Nazioni Unite sulle sfide e le misure per prevenire e combattere la corruzione e rafforzare la cooperazione internazionale tenutasi a giugno 2021 [33].

Il fenomeno corruttivo ha raggiunto dei livelli tali che non è più possibile, nella maggior parte dei casi, operare una distinzione tra ambito pubblico e ambito privato. Inquina, infatti, non solo le istituzioni minando la democrazia, ma al tempo stesso ha un forte impatto sulla vita delle imprese. A tal proposito, la Commissione europea ha più volte sottolineato la necessità di monitorare l'effetto che la corruzione ha sull'ambiente aziendale, motivo per cui le azioni anticorruzione sono annoverate tra le componenti importanti dei Piani di Risanamento e Resilienza.

Sino ad oggi il dato esperienziale relativo alla conoscenza della dimensione del fenomeno corruttivo emergeva a livello di percezione. L'organizzazione internazionale non governativa *Transparency International*, infatti, fornisce ogni anno i dati dell'Indice di Percezione della Corruzione, che dal 1995 costituisce il principale indicatore statistico del livello di corruzione percepita nel settore pubblico e nella politica in numerosi Paesi di tutto il mondo. Tuttavia, si parla appunto di percezione [34], mentre i dati reali soffrono di un difetto di conoscibili-

[33] Cfr. *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020DC0793&from=EN* e *https://ungass2021.unodc.org/ungass2021/en/information-on-ungass2021.html*.

[34] Cfr. AA.VV., *La misurazione della corruzione attraverso le sentenze: una proposta metodologica con strumenti di* text mining, in *Federalismi.it*, 2 dicembre 2020, pp. 169-70, che sottolineano l'*ontologica imprecisione* degli indicatori costruiti sulla percezione e da cui può scaturire il paradosso in base al quale «*un maggior livello di enforcement delle politiche anti-corruzione (repressive o preventive) è correlato ad un incremento del grado di percezione collettiva e individuale di questa fenomenologia criminosa in quanto motivato dalla maggiore visibilità* – rectius strepitus fori – *del fenomeno*». Si tratta del cd. *paradosso di Trogadero* su cui G. TARTAGLIA POLCINI, *Il paradosso di Trocadero*, in *Dir. pen. della globalizzazione*, 22 ottobre 2017, p. 1 ss.

tà dovuto alle giurisdizioni *off shore*, alla riluttanza di molti governi a monitorare la corruzione e all'assenza di dati.

Questo scenario sta rapidamente cambiando proprio grazie alle nuove tecnologie: la digitalizzazione degli appalti e la creazione di portali *online*, rendendo pubblici una grande quantità di dati su gare pubbliche, contratti e fornitori, ha restituito una visione più dettagliata del quadro corruttivo e delle sue relazioni causali [35]. *Big data* e *open data* alimentano strumenti automatizzati di monitoraggio con una potenza mai conosciuta prima, tanto da spingere la Commissione europea ad adottare alcuni strumenti operativi come l'*open contracting data standard* [36] (si tratta di una guida elaborata per segnalare ai governi i dati da pubblicare per rilevare i casi di corruzione), e la piattaforma *opentender* [37], che utilizza algoritmi di scansione dei dati forniti dai programmatori, incrociati con i dati provenienti da altri siti, in maniera tale da ottenere informazioni su gare di appalto aperte, storia e posizioni delle aziende che vi partecipano ed eventuali connessioni con il potere politico. L'interpretazione di tali dati restituisce indicatori di rischio di corruzione, che possono essere impiegati per sospendere una gara sospetta in previsione di un approfondimento di indagine e che potrebbe portare a chiedere ulteriori informazioni [38].

Dunque, il *data mining* può essere considerato l'arma principale dell'anticorruzione, date le sue caratteristiche di proattività basata sull'analisi dei rischi, la sua ripetibilità con conseguente difendibilità anche nello scrutinio del *post facto*. Ma non è sufficiente avere a disposizione una grande quantità di dati, quanto piuttosto è necessario possedere una buona conoscenza dei metodi di analisi e dei modelli decisionali e una conoscenza approfondita del *business* a cui i dati si riferiscono. Non è operazione semplice, infatti, estrarre i giusti indicatori dai dati e spesso può accadere che dall'analisi dei dati che misurano, ad esempio, la commistione tra corruzione e criminalità organizzata, emergano solo delle mere correlazioni di rischio [39].

[35] L. NANNIPIERI, *Il nuovo casellario informatico dei contratti pubblici di lavori, servizi e forniture*, in M. TRAPANI, *La prevenzione della corruzione. Quadro normativo e strumenti di un sistema in evoluzione. Atti del convegno*, Pisa 5 ottobre 2018, Torino, 2019, p. 187 ss.; E. BELISARIO, *Open Government e Open Data: la trasparenza e le nuove tecnologie come strategia per la lotta alla corruzione*, ivi, p. 197 ss.

[36] Cfr. A. PHETERAM, W. PASQUARELLI, R. STIRLING, *The next generation of anticorruption tools: big data, open data e AI*, in *Oxford Insight Research Report*, 2019, p. 4 ss.

[37] *Ibidem*.

[38] Sul ruolo dei *big data* nella misurazione della corruzione, si veda M. GNALDI, B. PONTI, *Misurare la corruzione oggi. Obiettivi, metodi, esperienze*, Milano, 2018, p. 90.

[39] Sul punto si veda AA.VV., *La misurazione*, cit., p. 168.

Fin qui i dati impiegati per l'analisi, interpretati per comprendere la portata dei fatti di corruzione. Il passo in avanti è costituito dall'utilizzo ulteriore di questi dati da parte dei programmatori come base per avviare e alimentare processi di apprendimento automatico dei sistemi di intelligenza artificiale, oltre che dall'impiego di reti neurali artificiali, che imitando il cervello umano nella sua capacità di stabilire connessioni, sono capaci di individuare relazioni, collegamenti e anomalie.

Oxford insights – organizzazione governativa con sede a Londra – sostiene la ricerca sulle nuove tecnologie proprio perché le considera la prossima frontiera dell'anticorruzione e i loro *partner* ritengono che la reperibilità dei dati non costituisca assolutamente un problema, dal momento che sono a diposizioni enormi *data set* provenienti sia da fonti governative (come appunto i sistemi fiscali ove trasparenti, i sistemi di appalti pubblici aperti, i registri pubblici), sia da altre fonti (oltre alla digitalizzazione di transazioni soldi e servizi, immaginate che ci sono 300 milioni di entità legali nel mondo i cui dati potrebbero essere incrociati, armonizzati e condivisi per scoprire casi di frodi, corruzione e truffe).

Semmai, i veri problemi al momento sono di due tipi. Da un lato, la capacità di armonizzare i dati e la mancanza di standardizzazione e condivisione degli stessi, dall'altro, la frammentarietà e la complessità del quadro normativo, che incidono sulla qualità dei dati e delle informazioni con il rischio di compromettere il processo di autoapprendimento dell'intelligenza artificiale.

Ed è su questo su cui bisognerà intervenire nell'immediato futuro, se si vuole impiegare questo tipo tecnologie nelle politiche anticorruzione.

C'è, poi, un ulteriore aspetto da valutare, ossia la capacità delle nuove tecnologie di svolgere una funzione di orientamento normativo. L'intelligenza artificiale, infatti, analizzando diversi *data set* può far emergere aspetti del fenomeno corruttivo che sono sin ora sfuggiti al legislatore indirizzando così le scelte di politica criminale. Non solo, ma riuscendo a collegare tutta la normativa di riferimento, permette di correggerla per renderla più efficace individuando anche eventuali lacune normative.

La casistica relativa all'impiego dei sistemi di intelligenza artificiale e delle reti neurali nel contrasto al fenomeno corruttivo non è ancora molto ampia e, per lo più, riguarda il riciclaggio e l'evasione fiscale; tuttavia, si possono già studiare alcuni usi o sperimentazioni che diversi paesi hanno portato avanti.

L'ambito di applicazione riguarda tre diverse ipotesi. Per i fatti già consumati, i sistemi di intelligenza artificiale possono essere impiegati nelle politiche pubbliche per le ipotesi di corruzione dei pubblici ufficiali o dei privati a danno della pubblica amministrazione. Si può, poi, fare ricorso a sistemi di reti neurali come strumenti predittivi, in grado di individuare una determinata area geografica a maggior rischio di fatti corruttivi. Da ultimo, in funzione di prevenzione dei rischi di corruzione, possono essere utilizzati dai privati nella *compliance*

aziendale, soprattutto per verificare la conformità dei modelli aziendali a normative e regolamenti.

Di quest'ultima ipotesi non ci sono ancora applicazioni in uso alle persone giuridiche e, dunque, bisognerà attendere i prossimi sviluppi per meglio comprenderne l'efficacia e le criticità.

Diversamente, per le ipotesi di scoperta e accertamento di fatti corruttivi consumati a danno della pubblica amministrazione, alcuni strumenti di intelligenza artificiale sono stati sperimentati in varie parti del mondo con risultati considerevoli, seppure in alcuni casi con criticità non superabili allo stato della tecnica[40].

Così è accaduto in Ucraina, paese considerato con il più alto livello di corruzione in Europa fino agli scandali del 2015 in cui furono coinvolti molti membri del governo. In quell'occasione furono introdotti due diversi tipi di strumenti: la piattaforma *Prozorro* e il *software Dozorro*[41]. Il primo strumento è stato ideato da un gruppo di attivisti e ONG internazionali e vi sono pubblicati tutti gli appalti pubblici per un totale di 1,67 milioni di gare pubbliche e un valore di 50 miliardi. Il secondo, invece, è un *software* che in una prima versione riusciva a far emergere fatti di corruzione in atto tramite l'analisi di 35 indicatori di rischio, con il limite che la pubblicazione degli indicatori permetteva alle strutture criminali di modulare le condotte corruttive, vanificando così il sistema. È stata adottata, allora, una nuova versione che non è vincolata a indicatori o formule prestabilite con un significativo aumento dell'efficienza dell'operazioni di indagine, il cui grado di precisione nel rilevamento dei fatti di corruzione è pari al 90%. A seguito dell'introduzione di queste tecnologie il paese ha visto diminuire grandemente il fenomeno corruttivo, scalando – così – numerose posizioni nella classifica di *Transparency International*.

4.4.1. *Il sistema cinese* Zero Trust

Nel contrasto alla corruzione, il sistema per eccellenza è sicuramente quello elaborato dalla Cina e che va sotto il nome di *Zero Trust*, la cui elevatissima efficienza è direttamente proporzionale alle criticità che pone. Entrato in funzione

[40] Cfr. P. AARVIK, *AI – a promising anticorruption tool in development settings?*, in *https ://www.u4.no/publications/artificial-intelligence-a-promising-anti-corruption-tool-in-development-settings.pdf*. L'autore offre un'ampia panoramica delle sperimentazioni in corso nel mondo strettamente connesse alla finalità anticorruzione. In Messico, ad esempio, il progetto *Open up Guides* monitora tramite l'intelligenza artificiale gli appalti pubblici, mentre in India il sistema *Project Insight* individua transazioni di alto valore, li confronta prima con modelli di spesa e poi con le dichiarazioni dei cittadini. Si tratta solo di alcuni esempi, ma per tutti l'aspetto problematico è la capacità di reazione una volta individuato il rischio di corruzione.

[41] Ancora A. PHETERAM, W. PASQUARELLI, R. STIRLING, *The next*, cit. p. 11 ss.

nel 2012 e sperimentato in sole 30 contee e città per una zona che copre l'1% dell'area amministrativa totale del paese, ha scoperto 8.721 casi di dipendenti pubblici coinvolti in fatti di corruzione, peculato, abuso di potere, indebita percezione di erogazioni pubbliche [42].

Il sofisticato sistema di intelligenza artificiale si avvale di centocinquanta database governativi allo scopo di monitorare l'operato dei funzionari pubblici, segnalando i casi in cui si raggiunge una predeterminata soglia di probabilità che sia in corso un fatto di corruzione. I dati impiegati sono molto eterogenei, si va da quelli bancari a quelli catastali, dalle proprietà mobiliari alle informazioni raccolte con le immagini satellitari [43], riuscendo a rilevare qualsiasi discrepanza tra lo stile di vita di un soggetto e il suo guadagno, tale da destare un sospetto di probabile corruzione. I risultati sono analizzati da funzionari con competenze in materia disciplinare, a cui spetta la decisione finale se indagare o meno il pubblico ufficiale.

Sembra il perfetto strumento anticorruzione, ma chiaramente non è così, tant'è che è stato sospeso.

Pur riuscendo a prevenire i fatti di corruzione nella pubblica amministrazione con una probabilità di successo pari al 72%, infatti, nessuno (né i programmatori, né gli inquirenti) è in grado di ricostruire il percorso di formazione delle prove, rendendole inutilizzabili in sede processuale. Non è solo un problema di *black box* come quello che si pone in generale per tutti i sistemi di intelligenza artificiale, ma è qualcosa di ulteriore e connesso all'enormità del numero dei dati utilizzati e alla complessità delle relazioni e connessioni tracciate dal sistema. Ciò costringerebbe gli inquirenti a un lavoro ulteriore di indagine per provare quanto è stato stabilito dalla macchina e non è detto che si riesca sempre a raggiungere il risultato, con un significativo dispendio di risorse.

Non solo, ma i funzionari della pubblica amministrazione hanno sofferto moltissimo la pressione psicologica del sentirsi costantemente monitorati anche nelle scelte di vita, nonostante le rassicurazioni del governo che lo scopo del progetto non è punire i funzionari, ma intervenire prima che le condotte corruttive siano portate a compimento. Nella maggior parte dei casi segnalati dall'intelligenza artificiale il pubblico dipendente sospettato ha mantenuto il posto di lavoro e ha ricevuto un avvertimento o nei casi più gravi una sanzione disciplinare, ciononostante la resistenza è stata tale che molti funzionari si sono rifiutati di fornire i dati necessari.

[42] V. C. BURCHARD, *L'intelligenza*, cit., *passim*.

[43] Il ricorso alle immagini satellitari serve non solo a verificare la zona di residenza del soggetto, ma anche ad assicurarsi che i soldi pubblici siano stati effettivamente impiegati per costruire un'opera pubblica prevista.

Tra le argomentazioni che hanno portato alla fine dell'esperimento e alla disattivazione del sistema, quella più pregnante ha fatto leva sulla violazione del principio di legalità, dal momento che manca nell'ordinamento cinese una disciplina *ad hoc* che autorizzi una simile tecnologia ad accedere a un *database* sensibile.

Anche la qualità dei dati utilizzati nell'addestramento dell'intelligenza artificiale ha posto molti problemi. Quegli stessi funzionari che monitorano i casi sospetti sono chiamati ad affiancare i programmatori nella fase di avvio del *machine learning*, fornendo la loro esperienza maturata in base ai casi precedenti e partecipando alla formazione dei *data set* con la segnalazione manuale di tutti i fenomeni che risultano essere insoliti. Dunque, il rischio che i dati siano fortemente viziati dai pregiudizi è molto elevato.

4.4.2. *L'esperienza spagnola: le cd.* mappe autorganizzanti

Rimane da analizzare l'ipotesi in cui le nuove tecnologie sono impiegate in funzione predittiva al fine di elaborare una previsione rispetto a possibili fatti di corruzione. Un esempio è costituito dalle cosiddette *mappe autorganizzanti*, elaborate dai ricercatori dell'Università di *Valladolid* in Spagna e valide per alcune aree geografiche, maggiormente esposte al rischio corruttivo [44].

Si tratta di strumenti che sfruttano la tecnologia delle reti neurali e dell'addestramento competitivo [45], secondo un modello matematico elaborato nel campo nelle neuroscienze computazionali e che prende le mosse dalla struttura del cervello umano organizzato in collegamenti tra neuroni. Dunque, una combinazione lineare di dati in entrata, organizzati in nodi o unità connessi tra loro mediante *link* e «*che prendono parte ad un processo noto come* winner takes all*, al termine del quale il nodo avente un vettore di pesi più vicino ad un certo input è dichiarato vincitore, mentre i pesi stessi sono aggiornati in modo da avvicinarli al vettore in ingresso. Ciascun nodo ha un certo numero di nodi adiacenti. Quando un nodo vince una competizione, anche i pesi dei nodi adiacenti sono modificati, secondo la regola generale che più un nodo è lontano dal nodo vincitore, meno marcata deve essere la variazione dei suoi pesi. Il processo è quindi ripe-*

[44] V. A. PETHERAM, W. PASQUARELLI, R. STIRLING, *The Next Generation of Anti-Corruption Tools: Big Data, Open Data & Artificial Intelligence. Research Report May 2019* Oxford Insights, in *https://static1.squarespace.com/static/58b2e92c1e5b6c828058484e/t/5ced49ccc8302518cb27f64b/1559054797862/Research+report+2019_+The+Next+Generation+of+Anti-Corruption+Tools_++Big+Data%2C+Open+Data+%26++Artificial+Intelligence.pdf*.

[45] L'acronimo è SOM, ossia *Self-organizing Maps*. Per un approfondimento tecnico si veda M.G. DI BONO, *Analisi comparativa di reti neurali autorganizzanti*, in *https://openportal.isti.cnr.it/data/2002/160553/2002_160553.pdf*, 26 settembre 2022.

tuto per ogni vettore dell'insieme di training, per un certo numero, usualmente grande, di cicli. Va da sé che ingressi diversi producono vincitori diversi. Operando in tal modo, la mappa riesce alfine ad associare i nodi d'uscita con i gruppi o schemi ricorrenti nell'insieme dei dati in ingresso. Se questi schemi sono riconoscibili, essi possono essere associati ai corrispondenti nodi della rete addestrata»[46].

Le mappe riescono a estrarre modelli di approfondimento da una enorme quantità di dati e anche quando non è possibile individuare alcun nesso logico, convertendo le relazioni non lineari in connessioni geometriche più facilmente identificabili, riescono a stimare la probabilità del verificarsi dei casi di corruzione. Il sistema permette di rilevare le criticità e indirizzare le azioni di monitoraggio e controllo, tenendo conto delle caratteristiche delle singole regioni, mentre un ruolo del tutto marginale è ascritto ai potenziali rei.

Nello specifico delle province spagnole in cui è stato testato il sistema, sono state individuate le variabili economiche e politiche che inducono la corruzione pubblica, come la tassazione immobiliare e l'aumento dei prezzi degli immobili, il permanere al potere dello stesso partito politico per lunghi periodi di tempo, una crescita economica troppo veloce o la crescita del numero di istituti di deposito. I dati sono contenuti in un archivio che raccoglie fattori macroeconomici e politici a partire dai casi che si sono verificati in Spagna tra gli anni 2000 e 2012 e che analizzati dalla rete neurale permettono di prevedere il rischio di corruzione negli appalti pubblici addirittura con 3 anni di anticipo sulla loro eventuale commissione.

Il modello può essere applicato anche ad altri paesi o regioni e potrebbe essere ritagliato sulle caratteristiche specifiche di ognuno di loro, con il risultato che i governi potrebbero utilizzare tali sistemi per identificare le vulnerabilità e indirizzare le azioni e i controlli in particolari aree a rischio.

4.5. *Lo strumento della* blockchain

Un altro strumento, generalmente associato alle monete virtuali, può fornire un contributo significativo per garantire la trasparenza dell'agire amministrativo e affiancare l'intelligenza artificiale nelle politiche anticorruzione. Si tratta della *blockchain*, una tecnologia altamente innovativa che, nella sua capacità di tracciare i dati e ricostruirne il percorso, garantisce proprio trasparenza e tracciabilità.

[46] Cfr. *https://digilander.libero.it/genio880/Mappe_auto-organizzanti_o_reti_SOM_(Self-Organizing_Maps)_1.htm*. In argomento, S. RUSSELL, P. NORVIG, *Artificial intelligence. A modern approach*, Edinburg, 2016, p. 727 ss.

Fino a prova contraria, il sistema non è modificabile né corruttibile in alcun modo e il suo primo impiego ha riguardato le monete virtuali come il *bitcoin*. Il suo utilizzo è stato esteso a molti altri usi, tra cui – e solo per citarne alcuni – la tutela delle banche dalle frodi sulle fatture o da qualsiasi altra forma di frode, per certificare qualsiasi forma di registro, per garantire filiere anche alimentari.

Tale strumento potrebbe contribuire al superamento del problema della mancanza di trasparenza nella pubblica amministrazione e che incide fortemente sulla efficacia degli strumenti anticorruzione. Con le dovute proporzioni, infatti, il dilemma della *black box* affligge da sempre anche la pubblica amministrazione italiana, nella misura in cui il rapporto con il cittadino è stato lungamente sbilanciato a favore dell'amministrazione statale e caratterizzato da opacità nei procedimenti. Il principio di trasparenza e buon andamento, pur essendo costituzionalizzato all'art. 97, solo in tempi più recenti ha trovato una affermazione in concreto; purtuttavia, permangono aspetti di opacità non altrimenti risolti e che contribuiscono significativamente alla pervasività del fenomeno corruttivo. La *blockchain* può svolgere un duplice ruolo, sia in ambito pubblico, sia in quello privato della compliance aziendale. Il sistema, infatti, concorre ad aumentare la trasparenza e la verificabilità dei dati nella pubblica amministrazione, contribuendo a realizzare la piena partecipazione dei cittadini ai processi decisionali delle istituzioni pubbliche. Al contempo può essere impiegata nei processi interni alle organizzazioni aziendali, certificando tutte le azioni intraprese e fondando dei modelli di organizzazione che inducono *best practice*.

Nelle esperienze di alcuni paesi in via di sviluppo, la cui vita democratica era fortemente condizionata da fatti corruttivi, corruzione elettorale, appropriazione indebita di fondi pubblici e finanziamento illecito ai partiti, la *blockchain* ha fornito un'occasione di svolta. Ha permesso, infatti, di costruire un unico registro in cui sono tracciate e conservate tutte le transazioni delle attività pubbliche, condiviso da tutte le pubbliche amministrazioni e, soprattutto, visibile a tutti, garantendo forme di controllo ulteriore del flusso di denaro pubblico [47].

La gestione della *blockchain* potrebbe, poi, essere affidata a un'Autorità autonoma, che garantisca l'indipendenza del sistema.

4.6. *Il difficile contemperamento tra tutela e progresso*

In Italia, l'*ex* presidente dell'ANAC – Raffaele Cantone – ha dichiarato che la predisposizione di mappe della corruzione in Italia dovrebbe addirittura esse-

[47] Cfr. A.I. SANKA, R.C.C. CHEUNG, *Blockchain: Panacea for Corrupt Practices in Developing Countries*, *2019 2nd International Conference of the IEEE Nigeria Computer Chapter* (NigeriaComputConf), 2019, pp. 1-7.

re una priorità delle politiche anticorruzione [48]. Si potrebbe, dunque, ricorrere alle reti neurali utilizzate per costruire le mappe autorganizzanti che, comportandosi come vere e proprie mappe topografiche avanzate, offrono una prospettiva più ampia e sono capaci di rilevare connessioni non sempre evidenti.

Benché il dibattito sulle nuove tecnologie abbia raggiunto un livello abbastanza avanzato [49], nel nostro paese ci sono ancora molte resistenze anche solo a testarle proprio nell'ambito del contrasto alla corruzione.

La legge Severino ha recepito l'importanza della raccolta dei dati, su cui è anche fortemente centrato il Piano triennale per l'informatica nella PA e della trasparenza oggetto del d.lgs. n. 97/2016 [50]; tuttavia, non c'è traccia di alcun riferimento all'impiego di nuovi sistemi nel Piano triennale di prevenzione della corruzione e della trasparenza dell'Autorità anticorruzione presentato a maggio 2021.

Senza dubbio le cautele osservate trovano una giustificazione legittima in quei limiti ontologici delle nuove tecnologie di cui si è detto in precedenza, costituiti dal difetto di trasparenza, spiegabilità e interpretazione dei sistemi e dai *bias*, che pongono a rischio alcuni diritti fondamentali. La posizione garantista, dunque, è senz'altro condivisibile quando in gioco ci sono i diritti fondamentali, ma a ben vedere alcuni di questi limiti sono superabili, permettendo un'apertura almeno a forme di sperimentazioni e valutazioni del rapporto costi/benefici.

Bisognerebbe ricordare, ad esempio, che il problema dei *bias* non si pone solo con le macchine, ma investe anche la decisione del giudice e il potere regolatore del legislatore [51]. Le argomentazioni logiche poste a fondamento di una sentenza, infatti, sono il frutto del procedimento di autoapprendimento che si ali-

[48] Cfr. G. DE BLASIO, A. D'IGNAZIO, M. LETTA, *Predicting Corruption Crimes with Machine Learning. A Study for the Italian Municipalities*, in *https://web.uniroma1.it/disse/sites/default/files/DiSSE_deBlasioetal_wp16_2020.pdf*, 2020, 16, p. 2 ss.

[49] Sono stati prodotti diversi documenti, tra cui le *Proposte per una strategia italiana per l'intelligenza artificiale*, elaborata dal Gruppo di Esperti MISE sull'intelligenza artificiale, in *https://www.mise.gov.it/images/stories/documenti/Proposte_per_una_Strategia_italiana_AI.pdf*; il Libro bianco per l'intelligenza artificiale, in *https://libro-bianco-ia.readthedocs.io/it/latest/*.

[50] Si tratta del decreto legislativo recante *revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione pubblicità e trasparenza correttivo della legge 6 novembre 2012, n. 190 e del decreto legislativo 14 marzo 2013, n. 33, ai sensi dell'articolo 7 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche.*

[51] Sul tema M. VERSIGLIONI, *Diritto matematico*, Milano, 2020, p. 233, osserva che il complesso di norme che forma l'ordinamento giuridico e tutte le procedure che ne conseguono sono il frutto di un procedimento algoritmico, in cui l'uomo fornisce gli *input* iniziali (il nucleo primigenio di norme) e su questo costruisce tutto il restante, senza che sia possibile espungere i pregiudizi propri di ogni mente umana. Così anche L. PALAZZANI, *Tecnologie dell'informazione e intelligenza artificiale*, Roma, 2020, p. 60 ss.

menta durante tutta la vita professionale del giudice grazie alla conoscenza e ai dati esperienziali. Che questi siano a loro volta inevitabilmente condizionati dai pregiudizi che ogni mente umana ha, è un fatto noto a tutto e che torna spesso alla ribalta della cronaca in occasione di verdetto evidentemente discriminatorio a causa dei pregiudizi delle giurie.

Nella società moderna l'antidoto è stato individuato nel principio di democraticità e nel pluralismo delle idee, tanto che non esiste un solo grado di giudizio e si prediligono organi collegiali. Parimenti, la stessa soluzione può essere adottata anche per il procedimento di autoapprendimento delle macchine, prescrivendo che la programmazione sia opera di un gruppo eterogeneo di persone piuttosto che di un solo programmatore, o addirittura immaginando un sistema da utilizzare per il controllo dell'altro. In entrambi i casi residua un margine di errore non altrimenti eliminabile e il cui rischio va accettato, a beneficio dell'evoluzione dell'umanità.

Di difficile soluzione appare, invece, il problema dell'impossibilità a ripercorrere il percorso decisionale della macchina, che pone significative difficoltà nella ricostruzione dell'impianto probatorio. Ciò comporta per gli inquirenti uno sforzo considerevole e ulteriore che non è detto porti a dei risultati, ma soprattutto può determinare un'attenzione investigativa selettiva, che concentra gli sforzi su determinati autori di reato, tralasciandone altri. Ne consegue anche il rischio di perdere di vista la centralità del fatto, o di assistere a una eccessiva anticipazione della soglia della punibilità.

Quanto detto, però, non dovrebbe portare ad assumere un atteggiamento di sfiducia e rifiuto rispetto agli svariati usi che la tecnologia può avere. Piuttosto, una posizione aperta alle sperimentazioni, si da testare gli strumenti e operare anche una verifica in termini di costi e benefici, potrebbe offrire un'importante occasione per un efficace contrasto proprio al fenomeno corruttivo, che tanto incide sulla tenuta del nostro sistema.

Emerge, allora, la stretta connessione tra le nuove tecnologie e il Diritto penale: le prime sono di ausilio e danno impulso al secondo [52], dal canto suo il Diritto penale è chiamato a impedire che l'intelligenza artificiale diventi uno strumento di potere e di minaccia, anche a dispetto dei suoi caratteri di *extrema ratio*, frammentarietà e sussidiarietà. Manca ancora, però, una visione condivisa sull'opportunità di adattare le categorie tradizionali alla nuova realtà o piuttosto superarle, a favore di scenari innovativi anche nell'ordinamento giuridico.

[52] Con tutto quello che ne consegue in termini di rischio di allontanamento dal fatto e determinismo penale come avveduta dottrina ha sottolineato. Si veda V. MANES, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in *Discrimen*, 15 maggio 2020, p. 13. Sul punto anche C. BUCHARD, *L'AI come fine del diritto penale? Sulla trasformazione algoritmica della società*, in *Riv. it. dir. proc. pen*., 2019, 4, p. 1909 ss.

Quale che sia la scelta, da un lato è necessaria una regolamentazione, sia tramite l'enunciazione di principi, al fine di tenere in conto il limite invalicabile del rispetto dei diritti fondamentali e l'importanza di mantenere la centralità dell'uomo, sia ricorrendo a una disciplina vincolante, che contribuisca a rendere certo il diritto di fronte alla pervasività di tali strumenti. Dall'altro, le scienze empiriche devono trovare spazio nelle politiche anticorruzione, costituendo *la precondizione per una scienza penale integrata* [53].

4.7. *Riepilogando*

Nella realtà odierna sembrano, allo stato, registrarsi due diverse velocità di approccio nella relazione con le nuove tecnologie. Da un lato, l'ordinamento giuridico con le sue comprensibili cautele e conseguenti lunghi tempi di gestazione, dall'altro, le grandi aspettative del mondo comune da cui scaturiscono soluzioni, progetti e sperimentazioni che modificano sempre più il vivere reale. Solo per citarne alcuni, c'è l'intelligenza artificiale soprannominata *Watson*, che ha cambiato il volto della pubblica amministrazione e delle imprese sudafricane, il progetto *Digiwhist* finanziato da Horizon 2020, che si serve di avanzati algoritmi per raccogliere enormi quantità di dati finalizzati a migliorare l'efficienza della spesa pubblica in tutta Europa, aumentare la trasparenza e combattere la corruzione, il sistema commissionato dalla Banca mondiale alla società *Microsoft* per rilevare le anomalie negli appalti pubblici tramite la combinazione di dati eterogenei.

Invero, non è facile tirare le fila del discorso. Alle volte sembra che le questioni sollevate rispetto all'implementazione, ai rischi e alla regolamentazione delle nuove tecnologie, siano da trattare come una realtà solo *aumentata*, per la quale sarebbe sufficiente applicare le stesse categorie e rafforzare gli strumenti esistenti [54].

Tutto sommato, i dati li abbiamo sempre trattati e le informazioni sono sempre state falsificate e manipolate, dunque, si tratta di una questione quantitativa e magari il Regolamento sulla protezione dei dati da un lato, e alcune fattispecie penali (esistenti o di nuova introduzione) dall'altro, possono tutelare dai pericoli anche l'*habeas data* che oggi viene contrapposto all'*habeas corpus*.

Come abbiamo introdotto la responsabilità delle persone giuridiche, possiamo introdurre anche la responsabilità della persona elettronica (magari non im-

[53] Così AA.VV., *La misurazione*, cit., p. 167.

[54] Cfr. XXI[st] International Congress of Penal Law, 2024 *"Artificial Intelligence and Criminal Justice"*, in *https://www.penal.org/en/information*.

piegandoci lo stesso tempo…)[55], come accettiamo di condividere molti aspetti della nostra vita personale sui *social*, possiamo accettare, anche se con molte cautele, i sistemi di riconoscimento facciale posti a controllo del territorio urbano[56].

Anche il problema della *black box* è, in parte, superabile se consideriamo tale anche la mente umana, per la quale, di fronte alla necessità di accertare il dolo, si parla di *probatio diabolica*. Alla stessa stregua i *bias*, per i quali numerosi studi hanno evidenziato come i colloqui di lavoro siano influenzati dai pregiudizi dei reclutatori umani quanto e forse di più delle macchine.

Altre volte, invece, prevale il pensiero che i rischi non siano a così basso impatto e le ricadute dell'impiego massivo delle nuove tecnologie sulla salvaguardia dei diritti umani possano essere tali da mettere in crisi la stessa tenuta del sistema.

Si è visto, ad esempio, come la manipolazione e l'alterazione dei dati e dell'informazione riesca a influenzare addirittura il consenso politico e come la capacità e velocità di diffusione rispetto all'enorme numero di persone che possono essere coinvolte, costituiscano di per sé un motivo sufficiente per ritenere il fenomeno diverso in termini di paragone da quelli appartenenti al passato: le *echo chambers* non sono proprio paragonabili ai circoli sindacali di un tempo.

Ecco il motivo per cui è importante il recupero della dimensione statale rispetto al controllo dei dati e non è auspicabile che siano i privati a mantenerne il potere regolatorio, né tanto meno il monopolio. Se è vero, infatti, che i dati nonostante la loro mole, non implicano necessariamente conoscenza, è pur vero che un loro uso indiscriminato e senza garanzie di qualità può alimentare quel rischio algoritmico che tutti temiamo.

Nell'ambito proprio del diritto penale i problemi che si agitano sono innumerevoli. Tra i tanti, delegare un concetto fondamentale come la pericolosità sociale a una valutazione robotica comporta il rischio di spostamento da un diritto penale del fatto a un diritto penale d'autore, un autore, però, la cui pericolosità non viene valutata sulla sua persona, bensì sugli indici probabilistici che ci fornisce la statistica. Ricorrere a strumenti predittivi ancora una volta incide sulla qualità di diritto penale centrato sul fatto, anticipato – invece – a un momento in

[55] Cfr. A. CELOTTO, *I robot possono avere diritti?*, in *BioLaw Journal*, 28 febbraio 2019, in *https://teseo.unitn.it/biolaw/article/view/1352*.

[56] Il tema è amplissimo e il dibattito fervido. Si assiste sempre più a una strumentalizzazione del concetto di sicurezza, che in tempi di rischio di attacchi terroristici, crisi economiche e pandemie, fa sempre più leva sul senso di paura della collettività e sulla conseguente richiesta di tutela. Ciò determina una sempre crescente e non consapevole compressione di alcuni diritti fondamentali, per il tramite delle nuove tecnologie, che portano all'introduzione di sistemi – ad esempio – di riconoscimento facciale anche di tipo emozionale, ancora molto discusse. V. S. ZUBOFF, *Il capitalismo della sorveglianza*, Roma, 2019.

cui il reato ancora non è stato compiuto, con conseguenti rischi di criminalizzazione che si autoavverano.

Non è da sottovalutare nemmeno il pericolo di deresponsabilizzazione degli operatori, che nel settore della giustizia potrebbe essere particolarmente evidente. Ove l'intelligenza artificiale, infatti, dovesse indicare una percentuale elevata di rischio, ad esempio rispetto a una valutazione di pericolosità sociale in tema di concessione di misure alternative, difficilmente un giudice deciderà in senso contrario. Si tratta del cosiddetto *effetto caprone* riferito in dottrina [57] e che potrebbe portare il potere giudiziario a decidere senza giudicare, alla stessa stregua di quanto avviene da tempo con la medicina difensiva, o anche a una giustizia esatta ma non necessariamente giusta [58]. Parimenti, in un futuro non troppo lontano qualcuno potrebbe invocare l'adempimento di un dovere *ex* art. 51 c.p. a seguito dell'esecuzione di una decisione algoritmica e ritenere, così, esclusa la sua punibilità.

Altrettanto rischioso è il caso in cui gli algoritmi, anziché essere usati in funzione di contrasto al crimine, divengono essi stessi strumento di perpetrazione di reati proprio come la corruzione, magari riuscendo a occultare quegli stessi dati e indicatori che sono oggetto di analisi computazionale da parte degli inquirenti [59].

La rivoluzione robotica a cui stiamo assistendo dovrebbe portare – ad avviso di chi scrive – a prediligere un approccio neutro al tema, per trarre benefici dall'enorme potenzialità che tali strumenti comunque stanno dimostrando di avere. Ciò implica la possibilità di un cambio di prospettiva anche rispetto a questioni ad oggi considerate immodificabili. Un risvolto positivo, ad esempio, potrebbe arrivare anche dall'accettare – con tutte le cautele e garanzie del caso – una forma legittima di giustizia predittiva, se questo possa evitare *ab initio* la lesione del bene giuridico [60] e contestualmente ridurre le ipotesi di ricorso al diritto penale, che riacquisterebbe la sua primigenia natura di strumento di *extrema ratio*. Una tecnologia che supporti l'azione di contrasto al fenomeno corruttivo non può che essere salutato con favore. Basti pensare che in alcuni paesi in cui è particolarmente evidente la corruzione giudiziaria, si è fatto ricorso all'intelli-

[57] A. GARAPON, J. LASSEGUE, *La giustizia*, cit., p. 155 ss.

[58] V. G. CANZIO, *IA, algoritmi e giustizia penale*, in *Sist. pen*., 8 gennaio 2021.

[59] Cfr. P. MORO, C. SARRA, *Tecnodiritto*, cit., p. 89. In qualità di strumento di reato, anche l'AI potrebbe essere oggetto di confisca o sequestro, così come prevede la Convenzione sulla corruzione del Consiglio d'Europa del 2005.

[60] Cfr. C. BUCHARD, *L'AI*, cit., p. 1909 ss., secondo cui il diritto penale può solo garantire la tutela dei beni giuridici in modo normativo e controfattuale, mentre il diritto penale dell'intelligenza artificiale rende impossibile o minimizza la lesione stessa.

genza artificiale per verificare, esaminare e controllare le prove utilizzate durante il processo, facendo emergere le eventuali contraddizioni dell'impianto accusatorio [61]. Secondo parte della dottrina, l'intelligenza artificiale contribuisce a realizzare la cosiddetta *open justice*, che rende la giustizia misurabile e trasparente, riducendo l'arbitrarietà dei giudici [62]. Sembra quasi la realizzazione del sogno di Beccaria, ma le perplessità su una simile capacità dei nuovi sistemi sono tante, proprio in virtù di quanto è stato sin qui esaminato.

L'umanità è, probabilmente, ancora in tempo utile per regolare la vita *onlife* [63] ed evitare il moltiplicarsi di rischi che imporrebbero al diritto interventi d'urgenza non risolutivi. Può venire in soccorso anche l'acquisizione sempre più diffusa del sospetto che l'intelligenza artificiale non sia poi così intelligente e che – al momento – la sua dipendenza dall'attività dell'uomo è tutt'altro che trascurabile. Da ciò scaturisce anche un'altra importante valutazione, relativa al significativo impatto che tali sistemi hanno in termini di sostenibilità ed erosione delle risorse [64]. L'impiego di questi strumenti, infatti, richiede grandi quantità di energia e pone non pochi problemi anche in termini di smaltimento e il tema diviene sempre più pressante in un momento storico in cui la crisi climatica sta mostrando gli enormi rischi e la fragilità dell'ambiente in cui viviamo.

A fare la differenza – ad avviso di chi scrive – sarà, dunque, il mantenimento di una visione antropocentrica, il rispetto dei diritti fondamentali e il ricorso a principi quali quello di precauzione e di stretta necessità e proporzione.

Si tratta di tre aspetti imperativi, strettamente connessi tra loro.

Il rifiuto di procedure interamente automatizzate e sottratte a qualsiasi controllo umano implica il necessario coinvolgimento non solo degli scienziati ma anche e soprattutto degli umanisti, chiamati a svolgere un ruolo fondamentale proprio nel processo di selezione dei dati molto più degli informatici o dei ma-

[61] Sul punto CUI. YADONG, *AI and Judicial Modernization*, Springer online, 2020, p. 22. L'autore illustra compiutamente il funzionamento del sistema in uso nei tribunali della città di Shanghai.

[62] *Ibidem*, pp. 38 e 40. L'*open justice* è un principio fondamentale degli ordinamenti di *common law* e ve ne è traccia già nella *Magna Charta*. In Australia le udienze sono visibili *online* e, quando è necessario opporre la segretezza – per esempio per fatti di terrorismo – la circostanza costituisce un motivo di criticità per il sistema, in termini di violazione di un principio fondamentale che non dovrebbe conoscere eccezioni. *Ex multis*, H. BURKHARD, A. KOPRIVICA HARVEY (a cura di), *Open Justice. The Role of Courts in a Democratic Society*, in *Studies of the Max Planck Institutes Luxembourg for international, European and Regulatory Procedural Law*, 2019.

[63] L. FLORIDI, *The Onlife Manifesto: Being Human in a Hyperconnected Era*, Springer, 2015.

[64] K. CRAWFORD, *Né intelligente né artificiale*, Bologna, 2021, p. 35 ss.

tematici. Dalla gestione virtuosa o meno dei dati dipende la potenza computazionale e la capacità predittiva, con la conseguente necessità di garantire la trasparenza degli stessi dati e, al contempo, la sinergia tra gli strumenti giuridici e quelli algoritmici.

L'introduzione di un obbligo di valutazione di impatto che preceda l'implementazione dei nuovi sistemi di intelligenza artificiale indipendentemente dal loro ambito di applicazione, può costituire un valido strumento di tutela dei diritti fondamentali sia nel settore pubblico, sia nel settore privato. Il ricorso a strumenti di monitoraggio e a organismi di sorveglianza, poi, può contribuire a garantire un buon livello di protezione, ma anche una maggiore condivisione e consapevolezza dell'importanza del tema nella collettività [65].

[65] Sul punto Agenzia europea per i diritti fondamentali, *Preparare un giusto futuro l'intelligenza artificiale e i diritti fondamentali*, Lussemburgo 2021, in *https://fra.europa.eu/sites/default/files/fra_uploads/fra-2021-artificial-intelligence-summary_it.pdf.*

CAPITOLO V

La responsabilità da reato dell'ente nel riciclaggio mediante monete virtuali

GASPARE JUCAN SICIGNANO

SOMMARIO: 5.1. Introduzione. – 5.2. L'interesse e il vantaggio. – 5.2.1. (*Segue*). L'interesse. – 5.2.2. (*Segue*). Il vantaggio. – 5.3. L'interesse e il vantaggio nel riciclaggio mediante monete virtuali. – 5.3.1. (*Segue*). L'interesse. – 5.3.2. (*Segue*). Il vantaggio. – 5.4. I modelli di comportamento. – 5.5. I modelli di comportamento nel riciclaggio mediante monete virtuali.

5.1. *Introduzione*

Secondo molti commentatori, il riciclaggio rappresenta il principale rischio connesso all'utilizzo delle monete virtuali. Molti utenti potrebbero acquistare le criptovalute con denaro di provenienza illecita e sfruttare le particolari modalità operative di questa nuova tecnologia informatica per ripulire il "denaro sporco".

Essendo questo lavoro dedicato alla responsabilità da reato degli enti nel caso di utilizzo delle monete virtuali a fini di riciclaggio, l'indagine verrà articolata in due parti: nella prima, si analizzerà il problema dell'interesse e del vantaggio dell'ente; nella seconda quello dei modelli di comportamento idonei a prevenire fenomeni di riciclaggio mediante criptovalute.

5.2. *L'interesse e il vantaggio*

Come noto, l'art. 5, comma 1, d.lgs. n. 231/2001 stabilisce che l'ente è responsabile per i reati commessi nel suo interesse o a suo vantaggio. Il concetto è ribadito dal comma 2 dell'art. 5, secondo cui «l'ente non risponde se le persone indicate nel comma 1 hanno agito nell'interesse esclusivo proprio o di terzi».

La nozione è molto controversa.

Deve innanzitutto ritenersi che i criteri di imputazione riferiti all'interesse e al vantaggio siano giuridicamente distinti giacché, mentre il primo è un criterio soggettivo, da valutare *ex ante*, e consistente nella proiezione finalistica volta a far conseguire all'ente un profitto indipendentemente dall'effettiva realizzazione dello stesso, il secondo è un criterio oggettivo, accertabile *ex post* e consistente nel concreto vantaggio derivato all'ente dal reato. La diversa opinione, secondo cui l'interesse e il vantaggio esprimerebbero uno stesso concetto, una sorta di endiadi, non sembra condivisibile. Senza voler qui riprodurre tutti gli argomenti addotti a sostegno della tesi "unitaria", basti solo ricordare che a quest'ultima conclusione si giunge grazie a una lettura congiunta del disposto dell'art. 5, u.c., d.lgs. n. 231/2001 e di quello dell'art. 12, comma 1, lett. a). Il primo prevede una esenzione da responsabilità della persona giuridica se il reato è stato commesso nell'interesse esclusivo dell'autore individuale o di terzi, il secondo un'attenuazione della sanzione pecuniaria nel caso in cui l'ente abbia commesso il fatto nel prevalente interesse proprio o di terzi e il vantaggio per l'ente sia minimo o inesistente. Secondo questa prospettiva, quindi, l'interesse risulterebbe essere l'unico criterio di collegamento davvero rilevante, mentre il vantaggio rappresenterebbe una sorta di variabile casuale, comunque non sufficiente ai fini dell'integrazione della responsabilità degli enti.

La tesi non appare condivisibile.

È necessario, invero, privilegiare una lettura della disposizione che consenta di evitare un'*interpretatio abrogans* del concetto di vantaggio. Inoltre, l'art. 12, comma 1, d.lgs. n. 231/2001 – prevedendo la riduzione della sanzione dell'ente solo nel caso in cui il reato sia stato commesso da una persona fisica nell'interesse esclusivo o proprio di terzi e l'ente non ne abbia ricavato vantaggio o ne abbia ricavato un vantaggio minimo – indurrebbe a ipotizzare che l'interesse potrebbe anche mancare, ma la responsabilità dell'ente ugualmente sussistere. Allo stesso tempo l'art. 5, comma 2, d.lgs. n. 231/2001, più volte richiamato dall'orientamento contrario, andrebbe letto in maniera diversa. Come evidenziato nella relazione ministeriale al d.lgs. n. 231/2001, «la norma stigmatizza il caso di "rottura" dello schema di immedesimazione organica; si riferisce cioè alle ipotesi in cui il reato della persona fisica non sia in alcun modo riconducibile all'ente perché non realizzato neppure in parte nell'interesse di questo. E si noti che, ove risulti per tal via la manifesta estraneità della persona morale, il giudice non dovrà neanche verificare se la persona morale abbia per caso tratto un vantaggio (la previsione opera, dunque, in deroga al primo comma)».

Ciò premesso, occorre ora definire nello specifico la nozione di interesse e quella di vantaggio.

5.2.1. (Segue). *L'interesse*

Come rilevato da parte della dottrina, deve esserne preferita una interpretazione in termini soggettivi del concetto di interesse, esprimendo questa nozione «una valutazione teleologica del reato, apprezzabile "ex ante", cioè al momento della commissione del fatto e secondo un metro di giudizio marcatamente soggettivo». Si deduce, pertanto, che, ai fini dell'imputazione della responsabilità dell'ente, «la persona fisica non deve aver agito contro la società» oppure che «tale interesse sia quanto meno coincidente con quello della societas». In questo senso si pone la relazione illustrativa al d.lgs. n. 231/2001, secondo cui «il richiamo all'interesse dell'ente caratterizza in senso marcatamente soggettivo la condotta delittuosa della persona fisica e che "si accontenta" di una verifica ex ante; viceversa, il vantaggio, che può essere tratto dall'ente anche quando la persona fisica non abbia agito nel suo interesse, richiede sempre una verifica ex post».

Per una diversa tesi, invece, l'interesse andrebbe interpretato in senso oggettivo, consistendo nell'attitudine oggettiva della condotta riconoscibile all'esterno. Si ritiene in particolare che dalla «condotta in sé e per sé considerata, inquadrata nel contesto della situazione concreta e valutata in una prospettiva ex ante, si dovrebbe poter inferire che l'autore individuale ha agito nell'interesse dell'ente». Quanto alla diversa tesi della natura soggettiva dell'interesse, si ritiene che questa teoria rischierebbe di determinare l'ingresso di fuorvianti tratti di atteggiamento interiore; in questo senso si è sostenuto che «l'illecito compiuto dall'autore individuale deve collocarsi in una prospettiva funzionale, di gestione degli interessi e di promozione delle attività che definiscono e circoscrivono il profilo di soggettività dell'ente collettivo».

Quest'ultimo orientamento non sembra condivisibile. Sembra logico opporre che, se si riconoscesse valore oggettivo anche all'interesse, non potrebbe più scorgersi alcuna differenza rispetto al vantaggio, ritornando così alla teoria unitaria, con tutti i problemi, evidenziati, che ne conseguirebbero. Inoltre, come rilevato, «il criterio di imputazione sul piano oggettivo non soddisfa (…) da solo il carattere personale della responsabilità dell'ente. Occorre qualcosa in più, e cioè che l'ente sia anche rimproverabile». Senza dimenticare che, sul versante della prassi giurisprudenziale, il criterio oggettivo dell'interesse o vantaggio sembra aver assunto un ruolo centrale rispetto al criterio di imputazione soggettiva, ovvero la colpa di organizzazione. Di conseguenza, il recupero dell'interesse in chiave soggettiva è l'unico modo per garantire il rispetto nell'ambito del sistema 231 del principio di colpevolezza di cui all'art. 27 Cost.

5.2.2. (Segue). *Il vantaggio*

Meno controversa è la nozione di vantaggio. Quest'ultimo criterio, come prima visto, assume una connotazione oggettiva e il suo accertamento non può non

avvenire mediante un giudizio *ex post*. Di conseguenza, «anche in assenza di un fine pro societate, la realizzazione di un vantaggio da parte dell'ente, come conseguenza della commissione del reato da parte di un soggetto idoneo a rappresentarlo, sarebbe dunque in grado di incardinare la responsabilità». Si discute, tuttavia, se rientri nel criterio in parola «il minimo e più casuale o effimero beneficio per l'ente, anche solo potenziale e di natura non patrimoniale» oppure sia necessario il verificarsi di un «vantaggio patrimonialmente quantificabile o economicamente apprezzabile». Quest'ultima tesi sembra preferibile, considerato che l'agire degli enti destinatari del d.lgs. n. 231/2001 è sempre un agire ontologicamente connotato dalla logica del profitto.

5.3. *L'interesse e il vantaggio nel riciclaggio mediante monete virtuali*

Ipotizzata la natura alternativa dei due criteri – dove l'interesse assume un rilievo soggettivo da valutare *ex ante* e il vantaggio un aspetto oggettivo accertabile *ex post* – ci si chiede se, nell'acquisto di moneta virtuale con denaro di provenienza illecita, rilevi un interesse dell'ente.

In senso critico, potrebbe obiettarsi che le criptovalute non sono patrimonialmente connotabili e, pertanto, l'acquisto di moneta virtuale non rientrerebbe nell'ambito dell'art. 5 d.lgs. n. 231/2001, che presuppone un interesse dell'ente a un arricchimento economico. Sulla scarsa valutabilità economica delle monete virtuali si è recentemente espressa la sezione specializzata in materia di impresa del Tribunale di Brescia. Il Tribunale è stato chiamato a decidere sulla legittimità della scelta di un notaio di non trascrivere una delibera di aumento di capitale di una s.r.l., sottoscritto in una criptovaluta. Secondo il notaio, la moneta virtuale utilizzata non era "suscettibile di valutazione economica" e quindi non era conforme al disposto dell'art. 2464 c.c., comma 2, a norma del quale «possono essere conferiti tutti gli elementi dell'attivo suscettibili di valutazione economica». Dello stesso avviso il Tribunale. Per il collegio la criptovaluta in questione «non è ad oggi presente in alcuna piattaforma di scambio tra criptovalute ovvero tra criptovalute e monete aventi corso legale, con la conseguente impossibilità di fare affidamento su prezzi attendibili in quanto discendenti da dinamiche di mercato». D'altronde, per molti le monete virtuali sono una bolla speculativa che presto esploderà, impoverendo tutti gli utenti. Per altri, le stesse sono «il più grande schema di Ponzi privato della storia». Si tratterebbe di una truffa, in cui si promettono forti guadagni alle vittime a patto che queste reclutino nuovi investitori.

Questa posizione non sembra convincente. Le monete virtuali non sono uno schema Ponzi e non sono una bolla speculativa. Al momento, nessun elemento certo induce a ipotizzare una tale conclusione. Molti esperti di finanza stanno

investendo nelle monete virtuali e quelli che oggi profetizzano la fine delle criptovalute sono gli stessi che negli anni '90 annunciavano la bolla di internet. Sappiamo tutti come è andata a finire. Internet ha conosciuto una diffusione sempre più rilevante, arrivando a controllare ogni aspetto della vita umana. In ogni caso, pur ammettendo la possibilità che l'*affaire criptocurrency* si risolva in una bolla, il problema è mal posto. Al fine di identificare l'interesse, non è necessario indagare se l'investimento sia redditizio, ma solo se *ex ante* la condotta risulti finalizzata a un arricchimento. E attualmente non può essere revocato in dubbio che l'acquisto di monete virtuali "a monte" rappresenti una operazione economicamente apprezzabile per chiunque. Ciò basta per farlo rientrare nell'ambito di operatività dell'art. 5, comma 1, d.gs. n. 231/2001.

5.3.1. (Segue). *L'interesse*

Alla luce di quanto appena evidenziato, è necessario ora verificare a quali condizioni possa rilevare un interesse dell'ente nel riciclaggio mediante criptovalute.

Ebbene, appare evidente che, alla luce di quanto sottolineato, la condotta non è sorretta da un interesse rilevante ai sensi dell'art. 5 d.lgs. n. 231/2001 tutte le volte in cui l'agente acquisti le *criptocurrency* per scopi personali. Se un amministratore di una società che si occupa di edilizia si procura criptovalute, con denaro di provenienza illecita, per acquistare una autovettura alla propria consorte, non agisce nell'ambito degli obiettivi e delle finalità della sua azienda. Di conseguenza, la vicenda non sembra riferibile all'interesse di cui all'art. 5 d.lgs. n. 231/2001. Discorso diverso si pone se il nostro amministratore acquisti monete virtuali, con denaro di provenienza illecita, e poi le spenda per acquistare beni e servizi utili all'azienda. In questo caso, l'acquisto di criptovaluta può rilevare ai fini della responsabilità degli enti.

In proposito, si pone un ulteriore problema: tendenzialmente, l'indirizzo a cui è collegato un determinato portafoglio di moneta virtuale è anonimo. È un mero elenco di cifre e non fornisce alcuna indicazione espressa sull'identificazione del suo proprietario. Di conseguenza, se in un determinato portafoglio c'è un quantitativo sospetto di criptovaluta, non è possibile, se si possiede solo l'indirizzo di riferimento, *prima facie* identificarne il proprietario. Pertanto, se gli organi inquirenti riescono a individuare un'operazione di riciclaggio compiuta mediante monete virtuali, avranno molte difficoltà a provare un collegamento tra la condotta e l'ente. Se, invero, la criptovaluta non è stata ancora spesa e giace in un portafoglio virtuale, indicizzato con un mero numero di serie, la persona fisica autore del reato potrebbe ben sostenere di aver agito per un interesse personale esclusivo. Il punto potrebbe anche rimanere senza alcuna smentita in sede processuale, risultando quasi impossibile provare il contrario.

5.3.2. (Segue). *Il vantaggio*

Occorre ora analizzare il vantaggio.

È appena il caso di sottolineare che l'indagine sul vantaggio assume rilievo concreto soprattutto nelle ipotesi in cui – per qualsiasi motivo – difetti l'interesse. Appare opportuno domandarsi se, nel riciclaggio mediante monete virtuali, possa ricorrere un vantaggio per l'ente qualora – dopo l'acquisto effettuato per un interesse esclusivo della persona fisica – maturi un successivo guadagno speculativo in favore dell'ente.

Negli ultimi anni, le criptovalute sembrano garantire notevoli guadagni, in conseguenza dell'incremento di valore raggiunto nell'ambito del tradizionale mercato di scambio. Si pensi al bitcoin. Negli ultimi anni, il valore di questa moneta virtuale non è stato mai stabile, registrandosi fluttuazioni sempre più significative. Nel 2011, il valore di un bitcoin è aumentato rapidamente da circa 0,30 dollari a 32 dollari, prima di tornare a 2 dollari. Durante la crisi finanziaria di Cipro, il prezzo dei bitcoin ha raggiunto 266 dollari, per poi ridursi poco dopo a circa 50 dollari. Il 29 novembre 2013, il costo di un bitcoin è salito a 1.224 dollari. Successivamente, è sceso a circa 200 dollari. A gennaio 2018 ogni bitcoin valeva 11.059,07 dollari mentre a febbraio 2021 ha raggiunto i 50 mila dollari. Oggi un bitcoin vale 36.989,46 euro. Nel 2030 ogni singolo bitcoin potrebbe toccare quota 500 mila dollari.

Potrebbe quindi ben accadere che – dopo l'acquisto effettuato per un interesse esclusivo della persona fisica – maturi un guadagno speculativo per l'ente, ma la soluzione al quesito deve essere comunque negativa: anche in questo caso, infatti, non può configurarsi responsabilità da reato degli enti perché l'illecito, pur tornando a vantaggio di questi costituisce un mero "vantaggio fortuito", non attribuibile in alcun modo alla volontà della persona giuridica. Come è noto, il "vantaggio fortuito" non rientra nell'ambito di operatività dell'art. 5, comma 1, d.lgs. n. 231/2001, ritenendosi in giurisprudenza che «in tema di responsabilità degli Enti, nel caso in cui l'operazione posta in essere dall'Ente abbia come effetto principale di aumentare i valori dell'attivo patrimoniale, anche se, nel complesso meccanismo realizzato, non possono essere esclusi risparmi sul piano fiscale, ricorre l'interesse dell'ente, diverso dal vantaggio che costituisce una sorta di variabile casuale, nei termini posti dall'art. 5, comma 2, D.Lgs. n. 231 del 2001 che ne esclude la responsabilità se le persone fisiche indicate nel comma 1 hanno agito nell'interesse esclusivo proprio o di terzi, circostanza questa che fa venir meno lo schema di immedesimazione organica, ragion per cui l'illecito commesso, pur tornando di fatto a vantaggio dell'ente, non potrebbe più ritenersi come fatto suo proprio. Questo perché se il vantaggio è "fortuito" non c'è responsabilità della Società non essendo attribuibile alla sua "volontà"».

5.4. *I modelli di comportamento*

Secondo quanto previsto nel d.lgs. n. 231/2001, l'ente, per non incorrere in responsabilità, deve avere adottato ed efficacemente attuato un modello organizzativo idoneo a prevenire la commissione dei reati previsti dalla normativa.

La norma distingue tra fatti commessi da soggetti in posizione apicale e fatti commessi da soggetti in posizione subordinata. Se ad agire è un soggetto apicale, l'ente non risponde se prova che: a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi; b) il compito di vigilare sul funzionamento e l'osservanza dei modelli curandone l'aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo; c) le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione; d) non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla lettera b). Se invece a commettere il reato presupposto è un soggetto subordinato, l'ente è responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza. Si precisa, inoltre, che è esclusa l'inosservanza degli obblighi di direzione o vigilanza se l'ente, prima della commissione del reato, ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi. I modelli inoltre hanno anche una funzione riparatoria: nel caso di una loro adozione *ex post*, l'ente potrebbe beneficiare di una riduzione della sanzione pecuniaria e dell'inapplicabilità delle misure interdittive. Lo scopo dei modelli è di ridurre – in maniera significativa – il rischio di commissione dei reati, indirizzando in modo virtuoso i comportamenti dei dipendenti e collaboratori, attraverso l'introduzione di presidi di controllo e di monitoraggio.

Le caratteristiche essenziali che i modelli devono possedere sono indicate negli artt. 6 e 7 d.lgs. n. 231/2001. Essi devono innanzitutto contenere una adeguata mappatura delle attività in cui è maggiormente radicato il rischio del reato e una disamina delle modalità attraverso cui tendenzialmente vengono commessi gli illeciti previsti dal d.lgs. n. 231/2001. È necessario, inoltre, prevedere protocolli che definiscano i processi decisionali e operativi dell'ente; individuare specifiche modalità operative funzionali alla gestione delle risorse finanziarie; predisporre flussi informativi nei confronti dell'organismo di vigilanza ("OdV"); nonché organizzare meccanismi di controllo interni con un articolato sistema disciplinare, anche predisponendo procedure che facilitino l'emersione dei comportamenti illeciti.

Come segnalato da attenta dottrina, sembra utile suddividere il modello in due parti: una generale e una speciale. Nella prima verranno indicati i sistemi di *goverance* e i sistemi organizzativi e di controllo della persona giuridica, oltre

alla dislocazione dei garanti e dei poteri, nonché le procedure di gestione dell'area amministrativa e contabile. La parte generale includerà, inoltre, il codice etico, le linee dell'attività di formazione, le modalità di rilevamento delle violazioni, la struttura del sistema disciplinare e l'istituzione, composizione e funzionamento dell'organismo di vigilanza. Nella parte speciale, invece, verrà descritta la struttura dei reati di riciclaggio, la mappatura delle attività a rischio reato, le funzioni aziendali coinvolte nelle aree a rischio, i principi generali di comportamento e il rinvio ai protocolli di gestione.

È necessario, in ogni caso, che la formazione e l'attuazione delle decisioni seguano il metodo protocollare, che prevede la predeterminazione del soggetto decisore, delle regole di decisione che questi deve seguire e dell'ordine in cui le regole stesse devono essere applicate. Le procedure devono essere caratterizzate dalla cd. "segregazione delle funzioni": colui che assume la decisione, colui che la esegue e colui al quale è affidato il controllo del processo devono essere diversi. È richiesta una precisa formazione del personale in merito alle linee di dipendenza gerarchica, alle procedure, ai flussi d'informazione e in generale a tutto quanto contribuisca a dare trasparenza all'operare dell'ente. I modelli devono essere dettagliati e non generici, risultando idonei laddove si caratterizzino per la loro concreta e specifica efficacia e per la loro dinamicità. Essi infatti «devono scaturire da una visione realistica ed economica dei fenomeni aziendali e non esclusivamente giuridico formale».

Per ridurre il rischio che la singola attività sia occasione di reato è comunque necessaria una dettagliata e specifica regolamentazione di ogni processo. In questa prospettiva, dovranno essere formalizzati i flussi informativi tra gli attori chiave del processo, nonché i flussi informativi nei confronti di tali organismi da parte dei responsabili funzionali. Occorrerà, inoltre, integrare e armonizzare i sistemi sanzionatori e disciplinari e prevedere uno specifico e articolato sistema formativo finalizzato a rendere effettivi i controlli nei processi operativi. Questi controlli richiedono competenze specifiche e sono demandati a tutti i protagonisti dell'organizzazione, in maniera più o meno ampia.

È discusso, inoltre, se devono essere adottati due diversi modelli: uno per gli illeciti commessi dai soggetti apicali e uno per quelli dei subordinati. Ad avviso di un primo orientamento «ferma l'identità di genus, il modello nel caso dei sottoposti avrà un contenuto diverso rispetto a quello indirizzato agli apici: deve infatti prevedere in relazione alla natura e alla dimensione dell'organizzazione nonché al tipo di attività svolta, misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio». Le matrici dei modelli sarebbero dunque due: una per gli illeciti commessi dai vertici e una per quelli commessi dai soggetti subordinati; questo soprattutto perché ogni modello è caratterizzato da una diversa disciplina, anche con riferimento all'onere della prova e all'obbligo di adozione. Questa

tesi non può, però, essere condivisa. Come evidenziato da altra dottrina, l'identità di funzione dei modelli comporta infatti l'esistenza di un unico istituto, caratterizzato da una disciplina unitaria, ricavabile dal complesso di norme in tema di modelli. Inoltre, le indicazioni strutturali contenute nell'art. 7 e nell'art. 6 sono perfettamente coerenti tra loro. Nella prassi, infatti, è stata accolta la tesi della unicità del modello, valido sia per gli illeciti commessi dagli apicali sia per quelli commessi dai subordinati. Come rilevato, «le indicazioni strutturali dell'art. 7 costituiscono un completamento e una specificazione di quelle più ampie contenute nell'art. 6, alla luce della sostanziale unitarietà del modello organizzativo, sia nella prospettiva funzionale/preventiva, sia in quella contenutistica/procedimentale».

Si ritiene, inoltre, che l'adozione dei modelli di comportamento sia un mero onere per l'ente e non un obbligo. In questo senso si è espressa la dottrina e la giurisprudenza maggioritaria, ritenendosi che l'adozione degli stessi sia necessaria nella misura in cui l'ente intenda giovarsi dei benefici che la legge collega all'istituto di cui agli artt. 6 e 7 d.lgs. n. 231/2001. La diversa tesi, favorevole alla natura obbligatoria dei modelli di comportamento non è condivisibile. Questa impostazione richiama i doveri di adeguata organizzazione che gravano *ex* art. 2381 c.c. sugli amministratori societari, nonché il dovere di controllo dei sindaci sull'adeguatezza dell'assetto organizzativo *ex* art. 2403 c.c. Si tratta tuttavia di meri obblighi civilistici che, al più, ricorrendone i presupposti, potrebbero fondare una responsabilità civilistica e non certo penalistica.

5.5. *I modelli di comportamento nel riciclaggio mediante monete virtuali*

Occorre ora comprendere quale contenuto specifico debbano assumere i modelli organizzativi e di gestione nel caso di riciclaggio mediante criptovalute. Generalmente, si può ipotizzare che in questo caso i modelli debbano intervenire – oltre che sui vari ambiti già citati in precedenza in relazione alla prevenzione del rischio di riciclaggio – su due aspetti specifici: l'anonimato garantito agli utilizzatori delle criptovalute e la tracciabilità delle varie operazioni.

Le monete virtuali, invero, garantiscono l'anonimato ai loro utilizzatori. Se spesso le varie transazioni sono interamente pubbliche e contenute in un database distribuito, l'indirizzo a cui è collegato un determinato portafoglio è generalmente coperto da uno pseudonimo. È un mero elenco di cifre e non fornisce alcuna indicazione espressa sull'identificazione del suo proprietario. Potrebbe ritenersi, quindi, che sia richiesto agli enti procedere alla necessaria identificazione di tutti coloro che abbiano partecipato all'acquisto della moneta virtuale, nonché di conservare i documenti, i dati e le informazioni utili a prevenire, individuare o accertare eventuali attività di riciclaggio. In questo senso si è già espressa la legge antiriciclaggio in relazione agli operatori in moneta virtuale.

La norma ha infatti ricompreso tra i soggetti obbligati il prestatore di servizi relativi all'utilizzo di valuta virtuale e il prestatore di servizi di portafoglio digitale. In quanto obbligati ai relativi adempimenti antiriciclaggio, gli stessi sono tenuti a una adeguata verifica della clientela (Titolo II, Capo I – artt. 17 ss.) e agli obblighi di conservazione dei documenti, dei dati e delle informazioni utili a prevenire, individuare o accertare eventuali attività di riciclaggio o di finanziamento del terrorismo (Titolo II, Capo II – artt. 31 ss.). Il punto potrebbe ritenersi conferente anche ai fini del d.lgs. n. 231/2001. Allo stesso tempo, potrebbe imporsi alle persone giuridiche di procedere alla segnalazione delle operazioni sospette, anche ai fini del d.lgs. n. 231/2001.

Questa soluzione, tuttavia, non convince.

Gran parte delle criptovalute non è anonima ma pseudonima. Questo significa che è possibile identificare l'autore di una determinata operazione, una volta svelato lo pseudonimo utilizzato. Basta, quindi, identificare la chiave pubblica di un determinato *wallet* per collegare la moneta virtuale a uno specifico soggetto. Numerosi studi recenti hanno elaborato diverse tecniche per scoprire gli utenti "nascosti dietro i bitcoin". Si pensi a BitIodine, una applicazione elaborata da tre studiosi italiani, che è in grado di individuare gli «indirizzi di cluster che potrebbero appartenere a uno stesso utente o a un gruppo di utenti, classific(ando) tali utenti e le etichette, e infine visualizz(ando) informazioni complesse estratte dalla rete Bitcoin». A risultati analoghi giunge un lavoro presentato da una équipe dell'Università della California. A ciò si aggiunga che, come appena visto, secondo la recente legge antiriciclaggio, i cambiavalute e i prestatori di portafoglio digitale devono procedere all'identificazione degli utenti. Se un ente acquista moneta virtuale rivolgendosi a un *exchanger* e detiene il relativo corrispettivo in un *wallet* digitale, l'identificazione degli utenti è già stata effettuata da questi operatori.

In ogni caso, è necessario intendersi. Se l'idoneità del modello è intesa come capacità di impedire la commissione del reato, è evidente che le misure imposte devono essere funzionali a questo scopo. Come evidenziato in dottrina, «l'indagine sui modelli deve essere condotta esaminando il loro ruolo all'interno della struttura dell'illecito». In questo senso anche la relazione al d.lgs. n. 231/2001, secondo cui l'ente deve adottare modelli di comportamento «specificamente calibrati sul rischio – reato, e cioè volti ad impedire, attraverso la fissazione di regole di condotta, la commissione di determinati reati (non tutti i reati, quindi, ma soltanto i c.d. reati presupposto)». Si aggiunge, infatti, che il modello deve essere specifico, evocando «la sua aderenza sostanziale rispetto al rischio da contenere» e richiamando «una connessione di scopo tra la regola cautelare e il tipo di rischio (a sua volta ben determinato) che si intende ridurre». Lo stesso accertamento del giudice sull'idoneità del modello deve averne ad oggetto proprio l'attitudine a prevenire la commissione del reato contestato.

Prendiamo in esame tre esempi: nel primo caso, l'ente acquista moneta virtuale con denaro provento di reato, rivolgendosi a un cambiavalute virtuale; nel secondo, acquista moneta virtuale con denaro provento di reato, rivolgendosi a un privato; nel terzo, l'ente vende moneta virtuale a un soggetto che l'acquista con denaro contante, pagandola a un prezzo ribassato. Nel primo caso, l'identificazione del cliente è già operata dall'*exchanger*, ai sensi della legge antiriciclaggio: pertanto, imporre analogo obbligo all'ente risulterà inutile e superfluo. Nel secondo caso, invece, nessun soggetto è tenuto all'identificazione dell'utenza. Ma lo svelamento dell'anonimato non risulta qui in grado di impedire la consumazione dei reati di riciclaggio: chi commette il riciclaggio è l'ente medesimo, che è già identificato. Anche in questo caso l'identificazione della controparte (colui che vende la moneta virtuale), evidentemente, è un'attività totalmente inutile. Discorso diverso per quanto attiene al terzo esempio, l'ipotesi in cui l'ente, per guadagnare un eventuale surplus, vende moneta virtuale, a prezzo ribassato, a un soggetto che ricicla denaro. In questo caso l'identificazione della controparte costituisce una attività necessaria per impedire la consumazione del riciclaggio.

Bisogna a questo punto procedersi alla segnalazione delle operazioni sospette, come prima ipotizzato?

La risposta corretta sembra essere di segno negativo, soprattutto perché non esiste un protocollo formalizzato con l'ente deputato a raccogliere la segnalazione secondo la legge antiriciclaggio, ovvero l'Unità di informazione finanziaria della Banca d'Italia (UIF). A ragionare diversamente, si richiederebbe solo di sovraccaricare un sistema già eccessivamente carico. Piuttosto, la segnalazione dell'operazione sospetta potrebbe essere sostituita dal rilevamento delle violazioni del modello. Si tratta di un onere già previsto in ogni modello comportamentale che si attua mediante una denuncia al proprio superiore o a un apposito organismo aziendale. Come rilevato, «l'adeguatezza e l'effettività del modello dipendono, tra l'altro, dall'esistenza di un efficace sistema di rilevamento delle violazioni, che permetta la tempestiva emersione delle trasgressioni dalle regole di comportamento, non soltanto nelle loro forme più gravi, ma anche quelle che si traducono in mere deviazioni da regole di compliance che, se non vengono immediatamente neutralizzate, potrebbero fomentare un clima di anomia, foriero, nel tempo, di conseguenze ben più rilevanti per la società». Questo modulo procedimentale potrebbe essere proposto, anche nel caso di specie, al fine di evitare il riciclaggio dell'ente mediante criptovalute.

Potrebbe ipotizzarsi, tuttavia, che, se per i vertici dell'ente non è necessario imporre – in alcuni casi – l'identificazione degli utenti e la segnalazione delle operazioni sospette, analoghi oneri risulterebbero invece necessari per i sottoposti. Si ritiene in dottrina che «ferma l'identità di genus, il modello nel caso dei sottoposti avrà un contenuto diverso rispetto a quello indirizzato agli apici: deve

infatti prevedere in relazione alla natura e alla dimensione dell'organizzazione nonché al tipo di attività svolta, misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio». Le matrici dei modelli sarebbero dunque due: una per gli illeciti commessi dai vertici e una per quelli commessi dai soggetti subordinati; questo soprattutto perché ogni modello è caratterizzato da una diversa disciplina, anche con riferimento all'onere della prova e all'obbligo di adozione. Questa tesi non può, però, essere condivisa. Come evidenziato, l'identità di funzione dei modelli comporta infatti l'esistenza di un unico istituto, caratterizzato da una disciplina unitaria, ricavabile dal complesso di norme in tema di modelli. Inoltre, le indicazioni strutturali contenute nell'art. 7 e nell'art. 6 sono perfettamente coerenti tra loro. Nella prassi, infatti, è stata accolta la tesi della unicità del modello, valido sia per gli illeciti commessi dagli apicali sia per quelli commessi dai subordinati. Come rilevato, «le indicazioni strutturali dell'art. 7 costituiscono un completamento e una specificazione di quelle più ampie contenute nell'art. 6, alla luce della sostanziale unitarietà del modello organizzativo, sia nella prospettiva funzionale/preventiva, sia in quella contenutistica/procedimentale». In ogni caso, pure per i subordinati si ritiene che lo svelamento dell'anonimato non ha alcuna incidenza sull'impedimento del reato di riciclaggio.

Discorso diverso per quanto attiene alla tracciabilità delle varie operazioni.

Generalmente, le transazioni in moneta virtuale sono pubbliche, in quanto contenute in un database distribuito liberamente accessibile. Chiunque può controllare chi ha ceduto una determinata moneta a Tizio o a Caio, e chiunque può scoprire anche il report storico di ogni transazione. Per i bitcoin, in particolare, l'insegnamento di Giovanni Falcone "segui il denaro e troverai la mafia" sarebbe applicabile in pieno, laddove ce ne fosse bisogno. È possibile controllare, infatti, senza particolari sforzi, quale portafoglio possiede un determinato bitcoin, e quale strada ha percorso una determinata valuta per arrivare a una determinata destinazione. Tuttavia, in alcune ipotesi, le monete virtuali sono potenzialmente in grado di recidere ogni collegamento dei proventi illeciti con il reato presupposto. Si pensi a un soggetto che acquisti un quantitativo di criptovalute con denaro contante, provento di reato. Se effettua la sua operazione rivolgendosi a un privato, senza ricorrere a un cambiavalute ufficiale, non è sottoposto ad alcun tipo di controllo e ad alcun obbligo di segnalazione. Potrebbe sostituire il denaro con le monete virtuali in maniera agevole, senza essere minimamente tracciato. Una volta completata l'operazione, nessuno potrà mai collegare la moneta virtuale con il reato presupposto. Il passaggio dal mondo fisico al mondo virtuale recide irrimediabilmente ogni legame. A nulla rileva l'eventuale generale tracciabilità della transazione, perché a monte, quando si verifica la sostituzione di denaro contante in moneta virtuale, l'operazione è anonima. In alcuni casi, inoltre, i riciclatori potrebbero adottare alcuni escamotage per dissimulare il proven-

to di reato. Potrebbero, ad esempio, caricare il denaro illecito su carte di credito prepagate e poi effettuare gli acquisti di moneta virtuale, in perfetto anonimato. Stesso discorso vale nel caso in cui si utilizzi una società off shore, che, dopo aver accumulato provviste di provenienza illecita, le converta in moneta virtuale attraverso exchanger sottratti agli obblighi antiriciclaggio. In questo caso, l'intera operazione potrebbe avvenire su indirizzi intestati alla stessa persona giuridica e poi rimbalzati su numerosi portafogli virtuali facenti capo ad altrettanti schermi societari, fino ad arrivare sul wallet della persona fisica che poi procede alla conversione e, quindi, alla "riemersione" nel circuito delle valute a corso legale.

Per prevenire questi inconvenienti è necessario che l'ente istituisca un capillare si sistema di tracciabilità delle varie risorse confluite al suo interno, eventualmente utilizzate per l'acquisto di moneta virtuale. Come si è notato, «il modello deve prevedere la creazione di meccanismi interni all'ente, diretti a garantire la tracciabilità dei flussi finanziari e l'imputazione del pagamento, esplicitando quanto indicato nella relazione governativa riguardo all'esigenza di individuare i fondi e le modalità di pagamento». E non rileva, inoltre, il fatto che *ex post* le monete virtuali garantirebbero una perfetta tracciabilità. Come evidenziato in giurisprudenza, l'idoneità del modello va infatti accertata *ex ante*, secondo il modello della prognosi postuma, valutandone caratteristiche strutturali che devono rispondere a requisiti di efficacia, specificità e dinamicità.

CAPITOLO VI

L'algoritmo e le neuroscienze: la chimera *per smascherare le menzogne?*

ANTONIO PAGLIANO

SOMMARIO: 6.1. Le premesse. – 6.2. Porte aperte o porte chiuse all'uso della prova basata su l'algoritmo? – 6.3. Le tecniche di *memory detection* e il processo penale. – 6.4. (*Segue*). Il test a-IAT. – 6.5. Le prime applicazioni giurisprudenziali: il nodo della scientificità del metodo. – 6.6. La nemesi. – 6.7. Il processo che verrà.

6.1. *Le premesse*

Se dall'inizio del secolo il processo penale ha conosciuto il progressivo ingresso della prova tecnologica come suo nuovo baricentro, di recente stiamo assistendo alla decisa irruzione di varie e inedite forme di intelligenza artificiale che, sulla scia dell'esperienze vissute oltreoceano, portano con sé il rischio di mutare profondamente l'essenza dell'accertamento giudiziale. Mentre si cercano, vanamente, soluzioni all'oramai cronico mal funzionamento del nostro sistema processuale, i rapporti tra l'intelligenza artificiale (d'ora in avanti IA) e giustizia penale sono divenuti oramai oggetto di grande interesse anche a livello internazionale. Il dibattito all'interno della letteratura scientifica alimenta riflessioni "trasversali" che, muovendo dal profilo del diritto penale sostanziale [1], legato a tipo-

[1] Come condivisibilmente osservato, l'impiego della Intelligenza Artificiale nella commissione di alcuni reati è una delle più significative sfide della post modernità. La velocità di trattazione di una enorme massa di informazioni, secondo logiche di apprendimento e di elaborazione che mutano a seconda del tempo e dell'oggetto ma che non necessariamente rispondono a logiche causali (vuoi dire che l'utilizzo della IA non risponde a logiche causali? Se è questo che vuoi dire, allora, che IA è?), può determinare la trasformazione della struttura del reato ed influire sull'elemento soggettivo dello stesso. Inoltre, si prospettano condotte lesive di interessi di rango costituzionale, che meritano protezione anche penale, ma che appaiono di difficile sussunzione in ipotesi attualmente tipizzate. Così G. SALVI, *Ragioni di un*

logie di reato e a sottostanti fenomeni criminali, inevitabilmente intercetta non meno rilevanti problemi processuali.

La tematica, infatti, usando una terminologia molto in voga, si palesa estremamente fluida e poliedrica [2].

In questa sede, in cui si proverà a non sviluppare solo riflessioni teoriche cercando al contrario di affrontare problemi applicativi già emersi nella prassi, concentreremo l'attenzione unicamente sul versante processuale, nel cui ambito si inserisce lo specifico tema della prova scientifica applicata all'IA, con il suo corollario delle problematiche connesse all'accesso delle parti all'effettiva logica di funzionamento, ai fini del controllo sia della legittimità della stessa nel processo, sia della attendibilità del risultato.

Operando una estrema schematizzazione, strumentalmente funzionale a circoscrivere il parametro dell'analisi che si vuole qui sviluppare, si può affermare che, guardando ovviamente anche oltre il panorama nazionale, l'utilizzo dell'algoritmo all'interno del processo può essere declinato in due diversi ambiti [3].

Il primo, già ampiamente radicato nelle corti americane, riguarda l'applicazione dell'intelligenza artificiale per misurare il rischio di recidivanza del condannato, ai fini della determinazione dell'entità della pena o di una misura alternativa alla detenzione [4].

In sostanza, l'apprezzamento di merito in ordine alla propensione dell'imputato a ripetere il delitto viene affidato a un algoritmo di valutazione del rischio [5], *Risk*

incontro, in *Intelligenza artificiale e giurisdizione penale, Atti del workshop organizzato dalla Fondazione Occorsio (19 novembre 2021)*, in *Sistema penale*, 13 giugno 2022.

[2] Fra i molti impieghi della IA nel processo, si annoverano quelli relativi alla giustizia predittiva, al profiling, all'organizzazione dell'attività giudiziaria. Si tratta di temi di grande importanza ma su di essi vi è ormai ampia consapevolezza e vi sono molte iniziative di ricerca e di applicazione. Meno esplorato, invece, è il campo degli effetti dell'impiego della IA sulla struttura del reato e sulla possibilità di effettiva punizione di condotte illecite, per difficoltà probatorie ma soprattutto per il non sempre facile rispetto del principio di legalità e dei suoi corollari. Per una ricognizione del fenomeno, si rinvia AA.VV., *Intelligenza artificiale e giurisdizione penale, Atti del workshop organizzato dalla Fondazione Occorsio (19 novembre 2021)*, cit.

[3] In termini generali, gli scenari che implicano l'utilizzo dell'IA e che sollevano questioni di diritto penale sono quattro: 1. le attività di *law enforcement* e, in particolare, le attività di polizia predittiva; 2. i cd. *automated decision systems*, che potrebbero essere impiegati anche all'interno dei procedimenti penali, sostituendo in tutto o in parte la decisione del giudice; 3. i cd. algoritmi predittivi, impiegati per valutare la pericolosità criminale di un soggetto, cioè la probabilità che costui commetta nuovamente un reato; 4. le possibili ipotesi di coinvolgimento di un sistema di IA nella commissione di un reato.

[4] Il *leading case* è identificato in *Wisconsin S.C., State v. Loomis, 881, Wis. 2016*; ma si veda anche *Indiana S.C., Malenchick v. State, 928, Ind. 2010.*

[5] *COMPAS*: acronimo di *Correctional Offender Management Profiling for Alternative Sanctions.*

Assessment Tools, elaborato da un *software* giudiziario, brevettato e prodotto da una società privata, che vanta il segreto industriale su codice sorgente, database e tecniche di elaborazione dei dati.

Questa specifica declinazione dell'utilizzo di un algoritmo, in quella che viene definita "*giustizia predittiva*", produce evidenti risultati pratici di semplificazione delle procedure e di tendenziale calcolabilità e uniformità delle decisioni, con considerevole risparmio di tempi e costi.

Ciò evidentemente spiega come mai, nonostante i rischi e le annesse manifestazioni di scetticismo dei giuristi con forti richiami alla cautela in merito al rispetto delle garanzie nella raccolta delle informazioni utili per la valutazione del rischio, si registra nel sistema statunitense un'impetuosa avanzata di tali tecniche informatiche di tipo predittivo [6].

Di converso, la comunità internazionale si sta particolarmente preoccupando di assicurare che l'utile arricchimento delle fonti informative del giudice e le predizioni del modello statistico-matematico si coniughino sempre con il nucleo epistemologico tradizionale delle garanzie del giusto processo [7].

In particolare, si sta cercando, da parte della cultura giuridica europea, di far prevalere un approccio che consenta l'accesso al processo penale soltanto di uno standard "debole" della intelligenza artificiale, che consenta all'uomo di mantenere comunque il controllo della macchina.

Le linee guida della Carta etica europea rimarcano il criterio della non esclusività del dato algoritmico per la decisione, che dev'essere viceversa riscontrato da ulteriori e diversi elementi di prova [8], garantendo così la tutela dei diritti fondamentali della persona, della non discriminazione, della trasparenza, equità e comprensibilità dei metodi di elaborazione dei dati informatici, della controllabilità dei percorsi di calcolo, della qualità e attendibilità scientifica del risultato.

[6] Come evidenziato da G. CANZIO, *Intelligenza artificiale, algoritmi e giustizia penale,* in *Sistema penale*, 2021 (testo riveduto dell'intervento svolto in occasione del Webinar organizzato dalla Fondazione Leonardo – Civiltà delle Macchine su "Processo penale e Intelligenza Artificiale" (20 ottobre 2020), le principali critiche si sono concentrate con riguardo al rischio di distorsioni cognitive dello stesso algoritmo, per l'opacità del database, per l'indeterminatezza del codice sorgente, per l'automatica implementazione del *software*.

[7] Si rinvia, ad esempio, alla "*Carta etica sull'uso dell'intelligenza artificiale nei sistemi giudiziari e nel loro ambiente*", adottata il 3 dicembre 2018 dalla Commissione europea per l'efficienza dei sistemi di giustizia – CEPEJ. In particolare, si è fissato il principio secondo il quale, la coerenza logica del calcolo algoritmico deve sempre essere verificata in un processo d'integrazione fra le misurazioni quantitative, ricche e imponenti, da esso offerte con il percorso cognitivo e decisorio del giudice, nel rispetto dei metavalori dell'ordinamento.

[8] Come, d'altra parte, già avvertiva la S.C. del Wisconsin nella sentenza *Loomis* (il *software* COMPAS «*… should be always constitute merely one tool available to a Court, that need to be confirmed by additional sound informations…*»).

Quanto invece alla seconda possibile declinazione processuale dell'uso di un algoritmo, essa attiene ad una particolare combinazione fra neuroscienza [9] e intelligenza artificiale sulla quale concentreremo la nostra attenzione.

[9] Il termine neuroscienze è stato utilizzato per la prima volta dal neurofisiologo statunitense Francis Otto Schmitt nel gennaio 1962. In quel periodo Schmitt raccoglieva alcuni eminenti studiosi del cervello presentando loro un progetto dal titolo *Neurosciences Research Program*, che aveva lo scopo di coordinare le ricerche di base sul sistema nervoso, a livello fisiologico, biochimico, genetico-molecolare, farmacologico, anatomo-istologico, patologico, per dar luogo a un nuovo corpo di discipline, le neuroscienze, caratterizzate da elevato interscambio, cooperazione, da obiettivi e strategie didattico-formative del tutto proprie. Il termine neuroscienze indica un gruppo di discipline scientifiche tra loro assai eterogenee, ma che condividono un fondamentale programma comune: quello di comprendere come il cervello renda possibili i fenomeni mentali ed i comportamenti umani, anche quelli più complessi e tradizionalmente considerati inaccessibili all'indagine scientifica. Fino a non molti anni fa i fenomeni mentali venivano considerati come entità accessibili alla sola indagine introspettiva. In quest'ottica la conoscenza del substrato biologico dei processi mentali era considerata non solo superflua ma addirittura inopportuna, poiché il rapporto che il soggetto intrattiene con il proprio vissuto prescinde completamente dalle funzioni cerebrali; si veda, in particolare S. DELLA SALA, N. BESCHIN, *Il cervello ferito*, Firenze, 2006, p. 256. I comportamenti umani erano considerati come il risultato di complicate interazioni sociali comprensibili solo alla luce delle influenze ambientali e contestuali. Si riteneva pertanto che solo l'ambiente e la società, e non ciò che accade dentro la mente e nella psiche dei singoli individui, potessero adeguatamente servire a spiegare come e perché un individuo si comporta in un certo modo (si veda A. PATERNOSTER, *Scienza cognitiva e diversità culturale*, in R. CATERINA, *I fondamenti cognitivi del diritto*, Milano, 2008, p. 239). Malgrado gli sforzi di una parte della comunità scientifica, questo modello continua ad esercitare una silenziosa influenza su molti uomini di legge e prevalentemente in virtù di tale substrato le neuroscienze vengono costantemente accusate di annientare la nozione di responsabilità penale per il solo fatto di svelare la natura biologicamente condizionata dell'azione. A differenza del contributo dei condizionamenti ambientali, quello dei fattori biologici e genetici non viene pacificamente accettato, bensì osservato con sospetto e comunque circoscritto alla presenza di eventuali impedimenti di natura patologica. Nei paesi di lingua anglosassone queste prospettive scientifiche hanno già avuto dei riflessi in campo forense dove si parla addirittura di neuro giustizia, si veda A. MCNEILL HORTON, L.C. HARTLAGE Jr., *Handbook of forensic neuropsychology*, New York, 2003; S. ZEKI, O. GOODENOUGH, *Law and the brain*, Oxford, 2006. Ebbene non può negarsi che la genetica comportamentale, la socio-biologia, la psicologia evoluzionistica e le neuroscienze cognitive hanno segnalato sperimentalmente delle correlazioni tra organismo e comportamento che fino a ieri erano sconosciute, tant'è che qualcuno ha parlato di rivoluzione neuroscientifica. Ecco allora che un tentativo di dare una definizione delle "neuroscienze giuridiche" è stato fatto da alcuni studiosi che hanno ritenuto che le stesse ricomprendano le più diverse ricerche neuroscientifiche aventi un'applicazione giuridica diretta o indiretta, precisando che esistono: le neuroscienze forensi, che si occupano della prova neuroscientifica nel processo, le neuroscienze criminali, ossia lo studio neuroscientifico del soggetto criminale, le neuroscienze normative e della cognizione morale, ovvero lo studio neuroscientifico del senso di giustizia e ragionamento morale; si veda L. SAMMICHELI, G. SARTORI, *Neuroscienze giuridiche: i diversi livelli di interazione*

Ci riferiamo a quella particolare metodologia finalizzata ad identificare la sussistenza nel soggetto di tracce di memoria, ovvero la "*memory detection*" [10]. Rinviando ad altra occasione il tema estremamente interessante della "*giustizia predittiva*", in questa sede si concentrerà l'attenzione su ciò che abbiamo indicato essere il secondo ambito di declinazione dell'uso dell'IA all'interno del processo penale, ovvero l'utilizzo delle tecniche di "*memory detection*".

Tuttavia, prima di approcciare in concreto quali siano allo stato le principali applicazioni, e le connesse problematiche, dell'utilizzo di un algoritmo nell'agone processuale, occorre preliminarmente comprendere, come dire in termini generali, quale sia il modo migliore per gestire correttamente l'accesso nel processo di questo tipo di *electronic evidence*, ovvero di ciò che può essere considerato un peculiare sottoinsieme della prova scientifica e tecnologica.

6.2. *Porte aperte o porte chiuse all'uso della prova basata su l'algoritmo?*

Sono ben noti i criteri enunciati nel 1993 dalla Corte Suprema statunitense [11], in base ai quali il giudice deve vagliare l'effettiva affidabilità di una teoria o un

tra diritto e neuroscienze, in A. BIANCHI, G. GULOTTA, G. SARTORI, *Manuale di neuroscienze forensi*, Milano, 2009, p. 17. Dunque le neuroscienze forensi si occupano dei dati neuroscientifici rilevanti ai fini della valutazione giudiziaria, in altri termini dell'idoneità delle teorie e delle metodologie della neuroscienza a costituire valida prova scientifica all'interno del processo; si vedano: C. BRUSCO, *La valutazione della prova scientifica*, in L. DE CATALDO NEUBURGER, *La prova scientifica nel processo penale*, Padova, 2008, p. 33; G. CANZIO, *Prova scientifica, ragionamento probatorio e libero convincimento nel processo penale*, in *Dir. pen. proc.*, 2001, 10, p. 1193; O. DOMINIONI, *La prova penale scientifica*, Milano, 2005; P. FERRUA, *Epistemologia scientifica ed epistemologia giudiziaria: differenze, analogie*, in L. DE CATALDO NEUBURGER, *La prova*, cit., p. 3 ss.; P. TONINI, *Progresso tecnologico, prova scientifica e contraddittorio*, in L. DE CATALDO NEUBURGER, *La prova*, cit., p. 49 ss.; P. TONINI, *Prova scientifica e contraddittorio*, in *Dir. pen. proc.*, 2003, 12, p. 1459 ss.

L'ipotesi di perizia sull'imputabilità si è imposta nella pratica come il principale ambito di utilizzo delle neuroscienze, con le prime apparizioni nelle aule di giustizia grazie alle prime sentenze, emanate dai tribunali di Trieste e Como, che hanno considerato specifici assetti genetici e disturbi del funzionamento cerebrale come elementi di riduzione dell'imputabilità del reo ed elementi per riduzione della pena. Occorre premettere che mentre la tradizionale perizia psichiatrica, basata sul colloquio clinico e sui test, porta a diagnosi soggettive, spesso controverse, le neuroscienze, evidentemente secondo i suoi cultori, introducono invece un elevato tasso di oggettività nella valutazione psichiatrico-forense, fornendo una descrizione più completa della sintomatologia e dei suoi correlati neurali e genetici.

[10] L. SAMMICHELI, G. SARTORI, "*Neuroscienze e processo penale*", in *Cass. pen*., 9, 2010, p. 361.

[11] Cfr. sentenza *Daubert v. Merrel Dow Pharmaceuticals*, Inc., 509 US 579 (1993).

metodo e di un *expert testimony*, ai fini della loro ammissibilità come prova scientifica nel processo: la controllabilità mediante esperimenti; la falsificabilità mediante test di smentita con esito negativo; la *peer review* della comunità scientifica di riferimento; la conoscenza della percentuale di errore dei risultati; infine, il criterio subordinato e ausiliario della generale accettazione da parte della comunità degli esperti.

In Italia, la Corte di Cassazione, nel condividere i *Daubert standard*, ne ha arricchito la portata, con riguardo alla fase della valutazione della prova scientifica da parte del giudice, aggiungendo i criteri dell'indipendenza e dell'affidabilità dell'esperto, l'ampiezza e il rigore del dibattito critico che hanno accompagnato la ricerca, le finalità e gli studi che la sorreggono, l'attitudine esplicativa dell'elaborazione teorica [12].

Ancor più che per quanto riguardi la prova scientifica sin qui conosciuta nel processo penale, rispetto alla prova legata ad una particolare applicazione di un algoritmo, appare ad esempio necessario comprendere come si possa assicurare che nei suoi riguardi possa trovare compiutamente spazio il diritto di difesa, ovvero come si possa garantire la possibilità di procedere alla sua confutazione piuttosto che all'esercizio del diritto alla prova contraria. D'altra parte, quale deve essere l'approccio del giudice non tanto e non solo nel momento della valutazione della prova ma soprattutto in quello della sua ammissione.

Come autorevolmente evidenziato, rispetto all'irruzione della scienza e della tecnologia nel crogiuolo dell'esperienza giuridica, l'approccio del giudice non può che essere più flessibile, quanto al controllo delle parti sulle modalità di assunzione della prova, alla *discovery* e al contraddittorio, nel momento e in funzione sia dell'ammissione che della valutazione della prova, e, dall'altro, più rigoroso quanto alla verifica di attendibilità del risultato probatorio.

Viene in mente in proposito un passo della Relazione al Progetto preliminare del nuovo codice di procedura penale del 1989, riguardante la portata dell'art. 189 c.p.p., in cui si legge che: «*È sembrato che una norma così articolata possa evitare eccessive restrizioni ai fini dell'accertamento della verità, tenuto conto del continuo sviluppo tecnologico che estende le frontiere dell'investigazione, senza mettere in pericolo le garanzie difensive*» [13].

Nell'intenzione del legislatore si coglie pertanto con chiarezza come il filtro fissato in tale norma risulti a maglie ben più strette rispetto a quello previsto dall'art. 190, comma 1, che, ai fini dell'ammissione della prova in genere, si limita a selezionare negativamente solo «le prove vietate dalla legge e quelle che manifestamente sono superflue o irrilevanti»: un filtro, inoltre, che è assistito da un

[12] Si veda, Cass., Sez. IV, 17 settembre 2010, n. 43786, *Cozzini*.

[13] Così G. CANZIO, *Intelligenza*, cit.

significativo rafforzamento del contraddittorio anticipato, "*per*" la prova, ancor prima che "*sulla*" prova.

Se allora il processo penale non può aprioristicamente lasciare fuori dalla porta l'utilizzo degli algoritmi, anche al fine di restituire al funzionamento della giustizia penale una più adeguata immagine di efficacia e qualità, esso non potrà che essere di volta in volta rimesso alla professionalità del singolo giudice il quale, a sua volta, deve impegnarsi per una costante implementazione del suo grado di *expertise* nei riguardi delle tecniche inferenziali del ragionamento e nella verifica degli schemi statistico-probabilistici, acquisiti con l'ausilio della tecnologia digitale e con l'apporto della robotica e della logica dell'IA [14].

6.3. *Le tecniche di* memory detection *e il processo penale*

Tornando all'utilizzo delle tecniche di "*memory detection*", val la pena di ricordare come per il nostro sistema processuale penale il racconto del testimone reso nel contraddittorio non ha bisogno di riscontri esterni. Esso deve, comunque, essere inserito nel contesto delle altre risultanze (ove queste sussistano) per un riscontro di credibilità e, se ritenuto fondato, può – anche da solo – motivare la sentenza, sempre che non sussistano altre prove. Se, per un verso, la scelta del legislatore trova la sua *ratio* nel pieno affidamento al principio del contraddittorio come metodo per la formazione della prova, per altro verso, tale scelta produce l'effetto di rendere il testimone una sorta di notaio di sé stesso, nei termini in cui egli racconta ciò che ha appreso e contemporaneamente certifica che il contenuto del racconto è ciò che egli crede vero.

La psicologia e le scienze correlate, in particolare le neuroscienze, ci stanno però mostrando sempre di più come la memoria sia una facoltà fallace sicché può accadere che, in perfetta buona fede, il testimone possa riferire i fatti in modo fortemente difforme dal loro reale svolgimento, con evidenti effetti sulla correttezza dell'accertamento di responsabilità dell'imputato.

Si affaccia lentamente la consapevolezza, grazie appunto alle scienze cognitive, che la memoria ha meccanismi specifici che vanno conosciuti se si vuole avere una valutazione attendibile dei resoconti dei testi [15]. Così come ci sono persone che sanno fare i calcoli a mente meglio di altre, ci sono testimoni che ricordano molto bene ed altri molto male.

[14] Auspicio formulate sempre da G. CANZIO, *Intelligenza*, cit., *passim.*

[15] Storicamente, una delle prime ricerche empiriche è stata quella condotta da Musatti che, nel 1930 circa, ha rilevato come l'accuratezza e completezza del ricordo di un gruppo di testimoni variava moltissimo.

La capacità di base di ricordare o meno non è mai oggetto di valutazione all'interno del processo in considerazione della citata scelta del legislatore di affidarsi pienamente al contraddittorio come metodo in grado di far emergere le lacune, le mancanze, gli errori di percezione del testimone. In sostanza, il sistema si affida all'assioma in virtù del quale il teste che sarà affetto da una scarsa capacità di ricordo sarà smascherato attraverso un corretto svolgimento dell'esame incrociato.

Invero, l'assunto su cui poggia la struttura del nostro sistema processuale accusatorio di cui si è appena fatto cenno, postula, evidentemente, che accusa e difesa svolgano correttamente l'esame incrociato e che comunque ne conoscano i meccanismi.

La prassi, tuttavia, ci insegna che non sempre ciò corrisponde al vero. Non di meno, un teste con scarsa capacità di ricordare quanto vissuto, se in buona fede, può assai facilmente apparire credibile ed uscire quindi indenne da un pur corretto esame incrociato [16].

D'altronde, le vere amnesie, che tecnicamente si chiamano amnesie lacunari psicogene, sono molto rare. Più frequentemente, si tratta di un impoverimento del ricordo dovuto alla mancanza reiterazione dello stesso; fenomeno che riguarda più frequentemente l'autore del fatto ma che talvolta afferisce anche al semplice testimone. La mancata ripetizione del ricordo determina un impoverimento del ricordo stesso, ma questa non si può considerare una vera amnesia [17].

[16] Il metodo migliore per comprendere la frequenza con cui la memoria umana commette errori consiste nell'analizzare situazioni nelle quali tanti testimoni vedono, e successivamente descrivono, la medesima scena. I casi giudiziari nei quali questo avviene non sono moltissimi, ma in queste situazioni si osservano delle diversità notevoli nel racconto da un testimone all'altro. Ci sono moltissimi fattori che riducono la precisione con cui il testimone ricorda. Ad esempio, l'elevata distanza di tempo, l'età del testimone, quante volte ha ripetuto il racconto, se ha sentito il racconto da altri co-testimoni, se è stato interrogato con metodi inadeguati dagli investigatori. Forse uno degli elementi principali che riducono l'accuratezza del ricordo è la confondibilità dell'evento che deve essere raccontato. Ad esempio, una pugnalata è un evento non confondibile, che viene ricordato molto meglio, a parità di tutto il resto, rispetto ad una conversazione casuale al bar. Ciò evidentemente in considerazione del fatto che di coltellate non ne abbiamo mai viste, mentre le conversazioni al bar sono cose che succedono ogni giorno. Parlando ad esempio dei riconoscimenti di persona, è stato dimostrato come gli errati riconoscimenti (tipicamente effettuati mediante il riconoscimento all'americana o mediante riconoscimenti fotografici) siano la fonte più frequente di errore giudiziario. Un riconoscimento all'americana dovrebbe partire, ad esempio, da come il testimone descrive verbalmente l'autore del crimine (es. 60 anni, calvo, con i baffi) e tutti i soggetti inseriti nel confronto dovrebbero avere queste caratteristiche. Raramente, però, questo criterio viene seguito.

[17] Ancora più delicato è il tema che concerne i racconti dei bambini. Uno dei parametri che influisce sull'accuratezza del ricordo è il grado di maturazione dei meccanismi della memoria umana. Nel bambino la capacità di memorizzazione diventa simile a quella dell'a-

Senza voler in alcun modo mettere in discussione il principio che debba essere il giudice il *dominus* della valutazione del testimone, potendo egli contare sull'esperienza e sul senso comune, non si può aprioristicamente tenere fuori dal processo l'utilizzo di strumenti in grado di offrire un supporto alla valutazione sulla attendibilità di chi ha reso dichiarazioni da cui si può direttamente ricavare l'innocenza o la colpevolezza dell'imputato.

Per quanto possa apparire un paradosso, se le nuove frontiere delle indagini scientifiche, partendo dall'esame del DNA fino ad arrivare a sofisticate metodologie come ad esempio la BPA, hanno occupato sempre più spazio nel panorama probatorio del processo penale degli anni duemila, la testimonianza continua e continuerà a rivestire un ruolo centrale nel processo penale rappresentando, forse proprio per questa ragione, l'unico ambito probatorio in cui il giudice non ammette "intrusioni".

Eppure, le scienze cognitive mettono a disposizione molti dati certi, utili a valutare la qualità di una testimonianza. L'utilizzo di questi dati però si deve scontrare con il convincimento degli operatori del processo che la testimonianza non rientri a pieno titolo fra le aree di indagine scientifica e che la sua valutazione possa fondarsi solo sulla intuizione e l'esperienza acquisita.

In realtà, il ricordo del fatto puro e semplice non esiste; un evento, per il solo fatto di essere percepito, viene automaticamente alterato dal "valore aggiunto" che gli impone il percettore; ogni deposizione ha una sua personalità e non vi possono essere testimonianze identiche [18].

Ciò che si presenta alla conoscenza del giudice non è mai la nuda verità, ma la verità ricostruita e filtrata attraverso la personalità dei testimoni, deformata dalle distorsioni dei meccanismi percettivi, dalle interferenze dei processi mnestici, dai pregiudizi e dagli stereotipi [19].

Gli esperti delle scienze cognitive, ad esempio, non mancano da qualche anno di far rilevare come il passare del tempo sia un aspetto che la giurisprudenza interpreta in maniera del tutto errata. L'accuratezza del ricordo che si riscontra a

dulto verso gli 11-12 anni. Prima dell'acquisizione minimale del linguaggio, però, il bambino non potrà riferire verbalmente quello che ha visto. Anche dopo i 3-4 anni il ricordo è molto limitato in termini di completezza ed accuratezza e molto influenzato dalla sua (limitata) conoscenza del mondo. Solitamente il giudice, soprattutto se il bambino è piccolo, si avvale di un perito per capire se il piccolo testimone può produrre una testimonianza valida. Inoltre, la precisione con cui si raccontano i fatti cambia molto se il comportamento da descrivere viene visto o è agito in prima persona dal testimone.

[18] Tra i primi studiosi in materia W.L. STERN, *Zur, Psychologie der Aussage*, Berlin, 1902, pp. 350-70.

[19] G. GULOTTA, *Strumenti concettuali per agire nel nuovo processo penale*, Milano, 1990, p. 118.

fronte di una significativa distanza temporale che separa l'accadimento dei fatti dalla testimonianza in giudizio, a parte casi particolarissimi, dovrebbe rendere la stessa poco attendibile, in quanto non si riferisce a percezioni dirette ma più spesso a rilettura della documentazione o ad altre situazioni.

6.4. (Segue). *Il test a-IAT*

Allo scopo di provare a limitare l'effetto distorsivo dei meccanismi percettivi, alcuni studiosi hanno messo a punto un test, denominato a-IAT, che si prefigge lo scopo di verificare se un soggetto rechi traccia mnestica di un determinato evento autobiografico [20], ovvero un metodo di verifica dell'esistenza di una specifica traccia mnestica nel soggetto esaminato. Esso consiste in una valutazione strumentale del contenuto della memoria, basata sulla registrazione dei tempi di reazione in risposta a frasi che descrivono eventi autobiografici. Se sono disponibili due ipotesi contrastanti relativamente ad una memoria autobiografica (come sempre succede in ambito giudiziario, dove esiste un'ipotesi accusatoria ed una difensiva), la metodologia identifica la memoria corretta con un elevato livello di precisione, basandosi su un fenomeno relativo all'organizzazione del sistema nervoso, chiamato effetto compatibilità: quando due concetti sono associati fra di loro nella mente/cervello del soggetto e condividono la medesima risposta motoria (ad esempio, premere lo stesso tasto) i tempi di reazione sono molto rapidi; al contrario quando due concetti non associati condividono la medesima risposta motoria i tempi di reazione diventano molto lenti. Per avere un'idea di quanto forte possa essere tale effetto si immagini di guidare un'auto con le gambe incrociate o una bicicletta a mani invertite. In tutti e due i casi si diventa molto lenti ed inaccurati, questo perché nel nostro sistema nervoso il piede destro è associato all'acceleratore, quindi il suo spostamento a sinistra, per comandare la frizione, determina una condizione di incompatibilità. Dalla maggior rapidità ed accuratezza del movimento si ricava pertanto la condizione compatibile, cioè quella più "naturale" [21].

Analogamente, nel cervello della persona sottoposta al test viene provocato un conflitto artificioso, che si riflette in un allungamento dei tempi di reazione; una sorta di cavallo di troia per entrare nella sua mente ed identificare qual è la memoria vera.

In altri termini, il nostro cervello è progettato per rispondere in modo veritie-

[20] G. SARTORI *et al.*, *How to accurately detect autobiographical events*, in *Psychological Science*, 19, 2008, pp. 772-80.

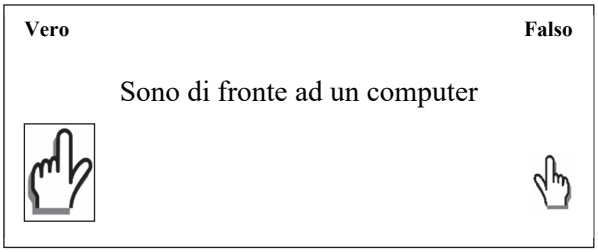
[21] G. SARTORI *et al.*, *How to accurately*, cit., pp. 772-80.

ro, ossia automaticamente produciamo una risposta veritiera; per produrre la menzogna dobbiamo bloccare, in modo efficiente, quello che spontaneamente ci viene in mente, e sostituirlo con una bugia; questa operazione richiede un tempo aggiuntivo, che viene misurato con lo a-IAT. La memoria vera viene riconosciuta perché può essere "raggiunta" più velocemente, mentre quella falsa ha un percorso cerebrale più "tortuoso" che si riflette in un allungamento abnorme dei tempi di reazione.

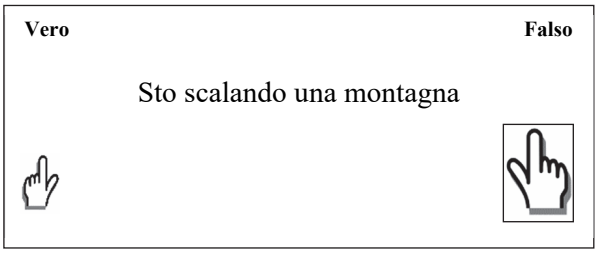
Ciò premesso, al soggetto da esaminare vengono proposte delle frasi che descrivono eventi biografici a lui riferiti. Il soggetto spinge un tasto "vero" o "falso" in base, appunto, al fatto che egli ritenga autentico o meno l'evento. In base ai tempi di risposta, un algoritmo valuta se ogni singola risposta fornita sia o meno associata a un ricordo custodito nella memoria.

Le frasi utilizzate sono suddivise in quattro categorie: frasi sempre "Vere" (ad es. "Sono di fronte al computer") e frasi sempre "False" (ad es. "Sto scalando una montagna") che riguardano il momento attuale; frasi dell'"Accusa" (per esempio "Ho ucciso mia madre"); e frasi della "Difesa" (per esempio "Non ho ucciso mia madre") concernenti la questione specifica; la prova complessiva viene spezzata in parti denominate "blocchi". Nel primo blocco appaiono, al centro dello schermo, frasi riferite al momento in cui il soggetto svolge il test. L'esaminato deve classificare queste frasi associandole ad una delle due categorie logiche ("Vero"/"Falso"), presenti rispettivamente a sinistra e a destra dello schermo ed associate ai due tasti di risposta.

Il soggetto preme il tasto sinistro per associare le frasi vere alla categoria VERO:



e il tasto destro per associare le frasi false alla categoria FALSO:



Il computer registra il tempo (in millisecondi) intercorrente tra la visualizzazione della frase e la risposta fornita dall'esaminato. La macchina viene così tarata sul singolo soggetto.

Questo compito, come quello del secondo blocco, ha anche la funzione di far conoscere al soggetto le frasi utilizzate e di "allenarlo" nel compito di discriminazione e classificazione.

Nel secondo blocco appaiono frasi riferite alle due versioni contrastanti associate all'evento autobiografico indagato (ad es. l'omicidio della madre). Le frasi descrivono, quindi, l'evento passato che il soggetto assume essere vero e che si deve indagare, nonché un evento alternativo che il soggetto assume non appartenere al suo vissuto autobiografico. Nell'uso forense del test, vengono costruite due ipotesi alternative, quella sostenuta dall'esaminato, che viene chiamata "ipotesi della difesa", e quella alternativa denominata "ipotesi dell'accusa", ciò al fine di comprendere se il soggetto abbia in memoria la versione che verbalizza o quella di cui è accusato. In questo secondo compito, all'esaminato non viene richiesto di classificare le frasi come vere o false, bensì semplicemente come corrispondenti alla ipotesi dell'accusa o della difesa.

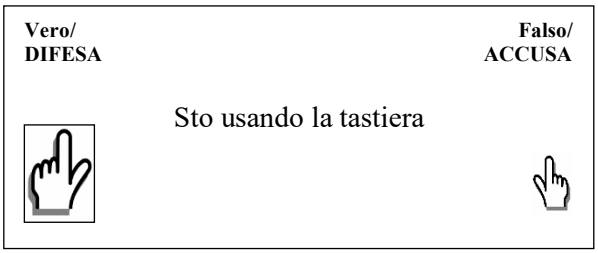
Nello specifico, l'esaminato deve classificare le frasi associandole ad una delle due categorie proposte (es. "Difesa"/"Accusa"), presenti rispettivamente a sinistra ed a destra dello schermo, associate ai medesimi due tasti di risposta del blocco precedente. Anche in questo caso il computer registra i tempi di risposta e tara il sistema. Il soggetto preme il tasto sinistro per associare le frasi riferite alla propria versione alla categoria DIFESA:

il tasto destro per associare le frasi riferite alla versione contrastante la propria tesi alla categoria ACCUSA:

Il terzo blocco unisce i due precedenti. Al centro dello schermo appaiono, una alla volta, sia le frasi riferite al momento in cui il soggetto svolge il test sia le frasi riferite all'evento indagato. L'esaminato deve associare le frasi riferite alla condizione al momento del test ad una delle due categorie logiche ("Vero"/"Falso") e le frasi riferite all'evento indagato ad una delle categorie "Accusa"/"Difesa".

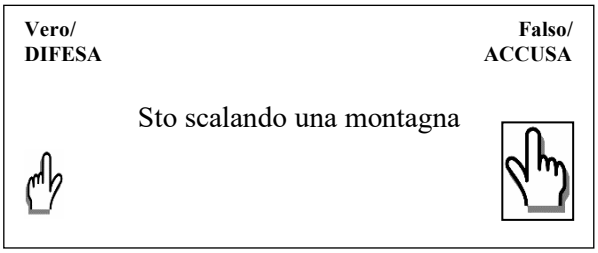
A sinistra del monitor sono presenti le categorie "Vero/Difesa", mentre a destra le categorie "Falso/Accusa".

Il soggetto preme il tasto sinistro per associare sia le frasi vere alla categoria VERO:



sia le frasi riferite alla propria versione alla categoria DIFESA:

mentre preme il tasto destro per associare sia le frasi false alla categoria FALSO:



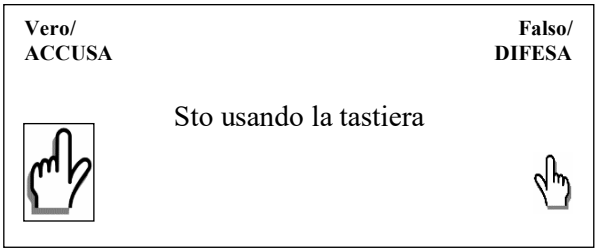
sia le frasi riferite alla versione contrastante la propria tesi e da associare alla categoria ACCUSA:

Il quarto blocco ripresenta lo stesso compito del secondo, invertendo, però, i tasti di risposta associati alle categorie ACCUSA e DIFESA. Le frasi visualizzate sono solo quelle riferite alle due versioni contrastanti ed associate all'evento indagato. Il soggetto preme il tasto sinistro per classificare le frasi da associare alla categoria ACCUSA ed il tasto destro per classificare le frasi da associare alla categoria DIFESA (vedi esempio secondo blocco).

Il quinto blocco costituisce un ulteriore blocco doppio, che unisce il primo ed il quarto. All'esaminato vengono presentate sia le frasi riferite al momento del test, da classificare con le categorie logiche "Vero"/"Falso", sia le frasi riferite alle due versioni contrastanti dell'evento indagato.

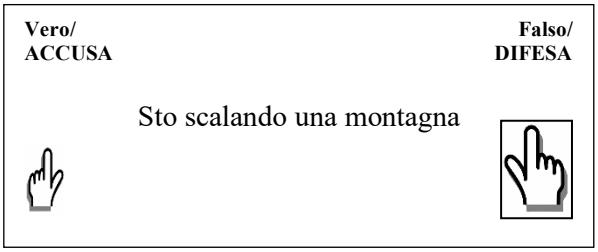
A differenza del terzo blocco, a sinistra del monitor sono presenti le categorie "Vero/Accusa", mentre a destra quelle "Falso/Difesa".

Il soggetto preme il tasto SINISTRO per associare sia le frasi vere alla categoria VERO:



sia le frasi riferite alla versione contrastante la propria tesi da associare alla categoria ACCUSA:

mentre preme il tasto DESTRO per associare sia le frasi false alla categoria FALSO:



sia le frasi riferite alla propria versione da associare alla categoria DIFESA:

Il terzo ed il quinto blocco, sicuramente più difficili per il soggetto, che deve continuamente passare da un criterio classificatorio all'altro, hanno lo scopo di creare un *conflitto cognitivo*. La mente umana, messa in questa condizione, tende ad abbinare implicitamente ed inconsapevolmente il concetto di "vero" alla memoria autobiografica effettivamente vera, e quindi fa meno fatica a classificare quando il tasto che rappresenta questi due concetti è lo stesso.

Di conseguenza, il computer registra una maggiore velocità di risposta nella classificazione.

Il senso di proporre al soggetto sperimentato il doppio abbinamento, a concetti invertiti, è proprio quello di metterlo in entrambe le condizioni: di abbinamento di "vero" con l'ipotesi d'accusa e di "vero" con l'ipotesi di difesa, per verificare quali dei due abbinamenti provoca la risposta più veloce.

In una delle due ipotesi vi è infatti un forte conflitto cognitivo, che ha come conseguenza un significativo rallentamento della risposta motoria, in quanto la mente deve effettuare un passaggio in più e quindi, un maggiore sforzo cognitivo, per poter classificare correttamente [22].

In questo modo, e grazie ad un apposito algoritmo che rende estremamente precisa l'analisi, la metodologia è in grado di verificare quale delle due versioni (accusa o difesa) *sia implicitamente associata al concetto di "vero"* nella mente

[22] Per una descrizione del metodo, si veda *http://aiat.psy.unipd.it/*.

del soggetto esaminato. Così, ad esempio, se il soggetto ha mostrato tempi di risposta minori in "Vero/Difesa", ciò significa che ha un'associazione molto forte, a livello di tracce mnestiche, tra il concetto di VERO e la categoria DIFESA, il che si traduce nella conclusione che l'ipotesi difensiva corrisponde al ricordo che l'esaminato ha dell'evento.

Esplicate le modalità di realizzazione del test, occorre provare a comprendere la sua utilizzabilità all'interno del processo e per procedere in questa direzione risulta di estremo interesse verificare quale sia l'origine di tale metodologia così da saggiarne il tasso di scientificità di cui gode.

Ebbene, in primo luogo occorre chiarire che il test a-IAT è una declinazione dello IAT che è stato teorizzato nel 1998 dal prof. Tony Greenwald [23]. La tecnica nasce e viene utilizzata per discernere propensioni inconsciamente razziste e discriminatorie nella popolazione. Questo è l'ambito di prevalente studio e applicazione del test, anche con potenziale rilevanza in ambito forense, ma in una declinazione assai diversa da quella che potrebbe avere in Europa perché attinente alla selezione della giuria popolare [24]. Infatti, tutta la ricchissima letteratura americana dedicata al tema degli *implicit bias* nell'attività delle corti e delle giurie dedica uno spazio speciale a tale metodologia proprio perché attraverso di essa è emersa la potente influenza degli stereotipi impliciti e delle attitudini implicite [25].

Come si diceva poc'anzi, la lettera "a" indica che il test di cui si discute rappresenta una variante, definita *autobiographical IAT*, del test IAT. La variante è stata costruita per valutare specificamente l'esistenza di una traccia mnestica del ricordo riferito dal soggetto.

Secondo i suoi ideatori, detta metodologia soddisfa i criteri per definire la pro-

[23] A.G. GREENWALD, D.E. MCGHEE, J.L.K. SCWARTZ, *Measuring individual differences in implicit cognition: The Implicit Association Test*, in *Journal of Personality and Social Psychology*, 74, 1998, pp. 1464-80.

[24] Si pensi alla potenziale utilità per selezionare una giuria: M.W. BENNETT, *Unraveling the Gordian Knot of Implicit Bias in Jury Selection: The Problems of Judge Dominated Voir Dire, the Failed Promise of Batson, and Proposed Solutions*, in *Harv. Law & Policy Rev*., 4, 149, 2010.

[25] Si rinvia agli studi di J. KANG *et al.*, *Implicit Bias in the Courtroom*, in *59 UCLA Law Rev.*, 1124, 2012; J.J. RACHLINSKI, S. JOHNSON, A.J. WISTRICH, C. GUTHRIE, *Does Unconscious Racial Bias Affect Trial Judges?*, in *Cornell Law Faculty Publications*, Paper 786, 2009. Ad esempio, sembra ormai consolidato che gli americani di razza bianca (ma anche quelli di razza nera, se pure in misura inferiore) esprimano una forte "white preference" allo IAT. Infatti, si è visto che associando una parola positiva ad un viso bianco e una parola negativa ad un viso nero i tempi di reazione sono più rapidi che operando le associazioni inverse. Cioè la latenza di risposta è maggiore quando il test propone una figura incongruente con lo stereotipo razziale. Dal pregiudizio razziale alla disparità di trattamento il passo è breve. Di qui, per l'appunto, gli studi rivolti a comprendere l'incidenza concreta del *racial bias* sull'amministrazione della giustizia.

va scientifica essendo accettata da parte della comunità scientifica e pubblicata su riviste mondiali *peer-reviewed*, non essendo falsificabile e presentando una percentuale di accuratezza del 92% [26].

Altro aspetto importante è costituito dal fatto che le analisi conseguenti alla somministrazione del test sono algoritmiche e questo significa che ogni consulente chiamato a valutare i risultati arriverà alle medesime conclusioni. La prova pertanto non è influenzata, nella fase di analisi, dall'abilità del consulente che effettua le analisi. Inoltre, il file prodotto automaticamente dal programma computerizzato alla fine della prova viene "fotografato" da un apposito algoritmo di sicurezza (lo stesso usato per le transazioni bancarie sicure) in modo da garantire l'assenza di manipolazioni. Il risultato finale è una "impronta digitale" del file che ha caratteristiche di unicità. Una modifica, anche minima, del contenuto del file verrebbe immediatamente identificata poiché il file non avrebbe più l'impronta digitale originaria rivelando così la manipolazione.

Questa procedura sembra effettivamente garantire che chiunque possa riverificare la correttezza delle conclusioni partendo dal dato originario non manipolato la cui integrità può, infatti, essere verificata in ogni momento. La fallacia del sistema, però, emerge nel caso in cui il soggetto sottoposto al test non intenda collaborare e fornisca risposte irrazionali, adducendo motivi di stanchezza ed emozione, paura o mancanza di ricordo. Si tratta di una casistica da cui deriva l'assoluta inutilizzabilità dei risultati del test stesso.

6.5. *Le prime applicazioni giurisprudenziali: il nodo della scientificità del metodo*

Ricostruite le concrete modalità di somministrazione del test e verificata la sua genesi oltre che le peculiarità, occorre interrogarsi sulla possibilità del suo concreto utilizzo all'interno del processo penale, non potendo certo ignorare come, nonostante la consolidata tendenza alla "scientificizzazione" dello stesso, in un ambito come quello della valutazione di veridicità della testimonian-

[26] L'accuratezza dello strumento in questione nell'identificare quale sia la associazione tra concetto ed evento autobiografico più forte è superiore al 92%. Ciò significa che su 100 casi esaminati, più di 92 vengono individuati in modo corretto G. SARTORI, S. AGOSTA, C. ZOGMAISTER, S.D. FERRARA, U. CASTIELLO, *How to accurately assess autobiographical events*, in *Psychological Science*, 19(8), 2008, pp. 772-80. S. AGOSTA, V. GHIRARDI, C. ZOGMAISTER, U. CASTIELLO, G. SARTORI, *Detecting fakers of the autobiographical-IAT*, in *Applied Cognitive Psychology*, 2010. Un elenco delle applicazioni pratiche può essere trovato nel sito dell'ideatore della tecnica il Prof. Tony Greenwald a questo link: *http://faculty.washington.edu/agg/pdf/37.Real-world_samples.21May2010.pdf*.

za, il giudice tende tradizionalmente a ritenersi del tutto autosufficiente.

In ogni caso, al di là della naturale resistenza all'ingresso nelle aule di giustizia della riferita tecnica di "*memory detection*" e non potendo certo ritenere la riferita metodologia d'indagine sulla autenticità di un ricordo autobiografico come consolidata, non si può prescindere dall'operare il già riferito accertamento del tasso di scientificità [27], verificando la validità e affidabilità del metodo scientifico quale premessa del ragionamento probatorio che si rifletterà poi sul procedimento argomentativo della sentenza [28].

Secondo taluni, se nei confronti delle discipline neuroscientifiche debbono considerarsi validi i principi generali concernenti la prova scientifica di cui si è poc'anzi fatto cenno, la peculiarità della prova neuroscientifica risieda in una maggiore dimostrabilità ed evidenziabilità a livello biologico dello stato di funzionamento patologico di funzioni mentali giuridicamente rilevanti [29]. A ciò si aggiunga poi che nel caso dello a-IAT, a quanto detto si associa l'uso di un algoritmo deputato alla elaborazione dell'esito finale del test, con gli annessi ulteriori problemi di verificabilità.

Negli anni passati il test in parola è stato introdotto in diversi processi, anche in taluni giudizi di revisione, con oscillanti esiti [30]. In solo due casi esso è stato infatti formalmente ammesso come prova e in un solo caso la sua utilizzazione ha influito nella decisione finale.

[27] La dottrina giuridica italiana si è in buona parte rifatta ai principi che regolano la materia nei sistemi giuridici anglosassoni. In tali ordinamenti i criteri da seguire per l'introduzione di esperimenti e tecniche scientifiche nel processo sono stati fatti oggetto di una nota elaborazione giurisprudenziale, che trova i suoi passaggi fondamentali nel caso *Frye vs. United States* (nel quale veniva fissato il criterio base della *general acceptance*) e nel caso *Daubert vs. Merrell Dow Pharmaceuticals* (nel quale venivano aggiunti al criterio precedente ulteriori canoni di verifica epistemologica: verificabilità della teoria, falsificabilità, controllo della comunità scientifica, la percentuale di errore noto o potenziale).

[28] C. BRUSCO, *La valutazione della prova scientifica*, in L. DE CATALDO NEUBURGER, *La prova scientifica nel processo penale*, cit., p. 38., individua la duplice attitudine della prova scientifica a fornire al giudice gli elementi per la ricostruzione del fatto e ad agevolare la valutazione della genuinità di altri mezzi di prova.

[29] L. SAMMICHELI, G. SARTORI, *Neuroscienze giuridiche: i diversi livelli di interazione tra diritto e neuroscienze*, in A. BIANCHI, G. GULOTTA, G. SARTORI, *Manuale di neuroscienze forensi*, cit., p. 25.

[30] Cass. pen., 2 gennaio 2013, n. 14255 proprio in tema di a-IAT (la decisione è inedita, ma è ampiamente richiamata nel contributo citato alla nota precedente). Successivamente, Cass. pen., 14 febbraio 2017, n. 13930. Per una completa ricognizione si rinvia a G. GENNARI, *Nuove e vecchie scienze forensi alla prova delle corti*, Santarcangelo di Romagna, 2016, oltre al più recente sempre G. GENNARI, *La macchina della verità si è fermata a Salerno…. fortunatamente*, in *Diritto penale contemporaneo*, 12, 2018.

Nel processo *Cogne bis*, ad esempio, ovvero quello in cui Annamaria Franzoni era imputata per la calunnia perpetrata nei confronti dei vicini di casa accusati di aver posto in essere l'omicidio del piccolo Samuele, i consulenti della difesa hanno utilizzato tale tecnica per stabilire se ella avesse o meno in memoria l'omicidio del figlio come fatto riconducibile ad una sua azione [31].

Il test ha rilevato la congruenza tra la rappresentazione verbale dei fatti fornita dall'esaminata e la traccia mnestica presente nel suo cervello: in altre parole, quella dell'imputata risultava essere una "memoria innocente".

Tuttavia, la prova, ammessa e ritenuta utilizzabile, non è stata valutata positivamente dal giudice che ha ugualmente ritenuto l'imputata colpevole per le false accuse pronunciate nei confronti dei vicini di casa.

Estremamente interessante si presenta la seconda vicenda giudiziaria di cui è stato protagonista l'uso processuale della tecnica in discussione, che, circostanza di estremo interesse, è stata introdotta per volere del giudice dell'udienza preliminare, che in sede di giudizio abbreviato, ai sensi dell'art. 441, comma 5, c.p.p. quale indagine integrativa, ha disposto una perizia allo scopo di verificare il racconto della persona offesa che aveva proceduto a formulare una denuncia di violenza sessuale nei confronti di un professionista presso il quale stava svolgendo uno stage. La particolarità che il test sia stato somministrato alla persona offesa e non all'imputato ha favorito la possibilità in capo al giudice di circoscrivere nel modo processualmente più corretto possibile il perimetro d'indagine del perito al quale è stato infatti richiesto di: «(…)*, valutato preliminarmente il ricordo dell'evento come potenziale causa di disturbo clinicamente significativo, verificare se la persona offesa, anche in considerazione della sua minore età e dello stato emotivo al momento del fatto, abbia subito un danno post-traumatico da stress o qualunque altro danno psichico riconducibile al reato denunciato. In questo caso ne chiarisca la natura, grado, durata e permanenza nel tempo*» [32].

Molto opportunamente, il giudice di Cremona non ha ritenuto di affidare al perito una generica verifica se la persona offesa avesse o meno raccontato il vero, quanto piuttosto una indagine volta a verificare, da un lato, se ella avesse dentro di sé il ricordo di quanto raccontato e, da un altro lato, se tale evento fosse stato potenziale causa di un danno post-traumatico da stress.

L'ammissione, l'utilizzo e la piena valutazione degli esiti della perizia, caratterizzano la vicenda processuale di Cremona come la prima in cui si è riconosciuta la piena scientificità del test di cui si discute, con l'ulteriore merito di aver saputo inquadrare il test in questione in quella che risulta, a giudizio dello

[31] Tribunale Torino, 19 aprile 2011, *inedita.*

[32] GUP di Cremona, 19 luglio 2011.

scrivente, la giusta dimensione probatoria, affermandosi in sentenza come «*tali metodologie nulla hanno a che vedere con gli antiquati tentativi di verificare la "sincerità" di un soggetto tramite lie detectors o poligrafi, strumenti che pretenderebbero di fondare la valutazione su grossolani sintomi psico-fisici del periziando* (…)», al contrario «*l'esame strumentale del ricordo autobiografico della ragazza ha permesso di identificare come proprio e "naturale" il ricordo corrispondente a quello descritto nell'accusa, costituendo una straordinaria conferma delle prove narrative che erano state raccolte nel corso dell'indagine*».

Una sorta di prova di riscontro avente ad oggetto la verifica della naturalità del ricordo di una determinata vicenda, in grado di rafforzare le risultanze già emerse in sede processuale. Lucidamente il giudice di Cremona ha posto in evidenza come, sebbene indubbiamente lo IAT non provi di per sé la verità storica di un fatto, esso è in grado di ricoprire il compito più limitato di far emergere, grazie ad una metodologia scientifica e controllabile e non in base ad apprezzamenti soggettivi, quale sia il "ricordo" cioè la "verità" propria di un soggetto in merito ad un determinato fatto [33], non potendosi escludere in linea di principio che il ricordo del soggetto sia comunque frutto di suggestioni, autoconvincimenti o distorsioni di quanto realmente avvenuto. Senza trascurare che la presenza di suggestioni o distorsioni della realtà, se riferiti a eventi semplici e determinati, comporterebbe comunque in capo al soggetto un certo grado di patologia, si direbbe di dissociazione dalla realtà, che non di meno il consulente che somministra il test è in grado di valutare, come puntualmente operato nel caso di specie in cui è stata esclusa la presenza di tali patologie.

La strada aperta dal giudice dell'udienza preliminare del tribunale di Cremone non è stata per nulla arata dalla successiva giurisprudenza che al contrario ha operato più di un passo indietro.

Nonostante infatti negli anni successivi si siano registrati diversi tentativi di utilizzo processuale dello a-IAT, essi sono stati sempre sostanzialmente frustrati [34], prevalentemente a causa della crescente conflittualità che si è registrata cir-

[33] Il GUP di Cremona, Dott. Guido Salvini, nelle motivazioni della sentenza di condanna del professionista ricorda come questa metodologia sia stata già usata in Italia, alludendo al processo satellite noto come *Cogne bis*.

[34] Si segnala in particolare, GIP di Venezia, 24 gennaio 2013, n. 296, in *Riv. it. med. leg.*, 2013, p. 1905 ss., con nota di L. ALGERI, *Accertamenti neuroscientifici, infermità mentale e credibilità delle dichiarazioni*; App. Catanzaro, 9 gennaio 2012, *inedita.* La sentenza è stata poi successivamente annullata dalla Cassazione proprio sul presupposto che la Suprema Corte ritiene lo IAT una valida metodologia sulla quale esisterebbe convincente letteratura, anche giuridica, si veda Cass. pen., Sez. V, 22 gennaio 2013, n. 14255, in CED. Investita del giudizio di rinvio, la Corte d'appello di Salerno boccia nuovamente lo a-IAT, affermando che il test IAT, utilizzato in psicologia sociale per valutare stereotipi, pregiudizi, atteggiamenti im-

ca il pieno riconoscimento della scientificità del test e ciò in conseguenza del fatto che la gran parte della letteratura citata a sostegno della sua validità proviene dallo stesso autore, o da suoi coautori, che quella tecnica la ha introdotta in Italia.

Si è poi posto in evidenza che tutti gli studi citati a supporto della validità scientifica e di cui in questa sede si è dato poc'anzi atto, si riferiscono solo allo IAT come strumento di misurazione di comportamenti potenzialmente discriminatori e pertanto non possono essere completamente traslati alla sua derivazione dello a-IAT. D'altronde, rispetto alla verifica del grado di scientificità del test in parola, ancora nei primi anni del duemila, rispetto al test IAT autorevoli voci della comunità scientifica americana sostenevano che esso fosse senza dubbio troppo immaturo per essere diffuso al grande pubblico o per essere utilizzato nelle aule dei tribunali [35]. Infine, si è sottolineato come la stessa percentuale di successo nel 92% sarebbe tratta dalla pressoché unica letteratura scientifica esistente che però proviene dallo stesso esperto somministratore del test [36].

6.6. *La nemesi*

Evidentemente non paghi dei crescenti rifiuti della giurisprudenza ad ammettere l'utilizzo del test che ha come protagonista la metodologia che intreccia le neuroscienze e l'uso degli algoritmi, non sono cessati i tentativi di ottenerne l'ingresso nell'agone processuale, registrandosi di recente una nuova tappa grazie a

pliciti verso prodotti di consumo o candidati politici, è cosa profondamente diversa dall'a-IAT che ricerca la traccia mnestica di un evento. Quello della memoria autobiografica è un concetto assai complesso con il quale interagisce l'auto-narrazione che il soggetto fa di un determinato accadimento, fermo restando, infine, che non sussiste alcuna validazione del metodo proposto in letteratura scientifica. Si veda, App. Salerno, 16 dicembre 2016, imp. Valenti, n. 2575.

[35] B. AZAR, *IAT: fad or Fabolous*, in *Monitor on Psychology*, 39, 7, 44, 2009; F.L. OSWALD, G. MITCHELL, H. BLANTON, J. JACCARD, P.E. TETLOCK, *Predicting ethnic and racial discrimination: A meta-analysis of IAT criterion studies*, in *Journal of Personality and Social Psychology*, 105(2), 2013, pp. 171-92.

[36] Così G. GENNARI, *La macchina*, cit., il quale a riprova della formulata considerazione evidenzia come La letteratura citata nella perizia sottoposta al GIP sia la seguente: G. SARTORI, S. AGOSTA, C. ZOGMAISTER, S.D. FERRARA, U. CASTIELLO, *How to accurately assess autobiographical events*, in *Psychological Science*, 19(8), 2008, pp. 772-80; S. AGOSTA, V. GHIRARDI, C. ZOGMAISTER, U. CASTIELLO, G. SARTORI, *Detecting fakers of the autobiographical IAT*, in *Applied Cognitive Psichology*, 2010. A questa si può aggiungere G. SARTORI, S. AGOSTA, *Menzogna, cervello e lie detection*, in *Manuale di scienze forensi*, cit., pp. 174-88.

una recente decisione della Corte di appello di Brescia [37]. Investita infatti di un ricorso di revisione nell'ambito del quale una delle tre nuove prove prodotte era rappresentata dagli esiti della somministrazione del test in parola [38], la Corte, allo scopo di sgombrare ogni dubbio, ha ritenuto opportuno procedere alla nomina di un perito al quale devolvere l'onere di stabilire se lo a-IAT sia buona scienza o meno.

Ebbene, il risultato della consulenza, che sembrava favorire la tesi dell'attendibilità della tecnica, affermando la sussistenza dei caratteri di scientificità, ne ha invece favorito la valutazione di non utilizzabilità, in applicazione degli artt. 188 e 64, comma 2, c.p.p., abbracciando pertanto una valutazione completamente opposta a quella formulata dal giudice di Cremona.

Procediamo per gradi. La perizia disposta dal giudice d'appello ritorna sulle conclusioni allora raggiunte e riconosce così al test in questione pieno valore scientifico.

Il perito ha chiarito che il metodo ha presentato una serie di modifiche e variazioni nel tempo dalla sua creazione e diffusione, modifiche che hanno riguardato prevalentemente la numerosità dei blocchi, passati da cinque a sette, e l'algoritmo utilizzato per il calcolo dei punteggi al test. Con riferimento a quest'ultimo elemento, si afferma che il nuovo algoritmo offre protezione dalla possibile precedente esperienza con procedura IAT. L'aver partecipato a una o più rilevazioni con detto metodo tende infatti a ridurre l'entità dei punteggi IAT successivi. La maggior robustezza e sensibilità del nuovo algoritmo potrebbe quindi migliorare I' affidabilità e il potenziale del metodo negli studi con più misure IAT o in caso di applicazioni che richiedono più fasi di testing.

Rispetto a quanto documentato dalla letteratura internazionale e nazionale, il test IAT presenta, a giudizio del perito, una base dati sistematica relativa ai criteri di attendibilità e validità. Con riferimento alla *validità*, il metodo si è mostrato efficace nel riflettere sia atteggiamenti impliciti universali – e quindi plausibilmente prevedibili –, sia atteggiamenti impliciti specifici che connotano peculiarmente alcuni gruppi di persone (come omosessuali o eterosessuali) e sensibile anche ad atteggiamenti impliciti acquisiti in tempi più recenti.

Quanto infine alle ricerche di letteratura sulla *attendibilità* del metodo, il medesimo perito ha affermato che un'ampia letteratura ha consentito di ricollocare la misura IAT tra le *misure di tipo implicito* con *maggiori valori di attendibilità*,

[37] App. Brescia, 15 luglio 2020 (dep. 11 novembre 2020), n. 1683, Pres. Deantoni, rel. Milesi.

[38] Giova ricordare che è oramai un principio consolidato in giurisprudenza che il medesimo fatto, apprezzato secondo tecnica scientifica non disponibile all'epoca del giudizio possa aprire le porte della revisione; si veda Cass., 2 gennaio 2013, n. 14255, *inedita* (fra l'altro proprio in tema di a-IAT); Cass., 14 febbraio 2017, n. 13930.

tanto che una recente meta-analisi ha calcolato e fornito i valori relativi alla "tenuta nel tempo" delle prove – ad esempio con specifico riferimento all'applicazione nello studio di casi di abuso sessuale.

Le conclusioni, con riferimento al metodo IAT sono, pertanto, nel senso che il metodo è definibile come una misura implicita e indiretta, validata e considerata come una misura oggettiva in grado di descrivere e predire atteggiamenti, attitudini e comportamenti relativi a situazioni ed eventi. Basandosi su indici associativi mediante rilevazione cronometrica, costituisce un valido strumento, come ampiamente riconosciuto dalla comunità scientifica internazionale.

Quello che tuttavia sembrava rappresentare il preludio per il definitivo "sdoganamento" della metodologia in discussione ha invece favorito la valutazione circa la sua non utilizzabilità; la Corte d'appello di Brescia ha ritenuto infatti che lo a-IAT, proprio in virtù di ciò che lo rende scientificamente riconosciuto, non può costituire prova utilizzabile, in conseguenza di due "effetti" evidenziati dalla perizia. Il primo è costituito dalla capacità del test di fare emergere memorie implicite, cioè memorie che siano inconsapevoli anche per il soggetto che si sottopone alla prova e ciò in considerazione della circostanza che secondo lo stesso ideatore del test, esso potrebbe fare emergere un certo ricordo, magari in qualche modo mistificato inconsciamente dalla persona, nella sua nitidezza ed anche al di là della consapevolezza del soggetto.

Il secondo effetto attiene invece alla capacità di smascherare le false versioni consapevoli e quindi di smascherare l'eventuale "imbroglione".

Il combinato disposto di questi due effetti, secondo la Corte, rende il test a-IAT del tutto analogo a una macchina della verità, il cui utilizzo è, come noto, vietato dagli artt. 188 e 64, comma 2, c.p.p., sconfessando così le argomentazioni formulate oltre dieci anni fa dalla sentenza del GUP di Cremona. Il test, si legge in sentenza, supera un limite invalicabile all'attività probatoria «costituito dal divieto di impiegare strumenti capaci di alterare la libertà di autodeterminarsi di ogni persona e, soprattutto, capaci di alterare la sua autonomia nel ricordare e valutare le cose», rendendo in sostanza lo a-IAT uno strumento troppo potente per essere utilizzato nel processo penale.

La Corte non lesina di approfondire la questione, affermando che sussisterebbe un duplice "vizio" processuale perché, da un lato, il consenso dell'imputato sarebbe prestato "a scatola chiusa", con una sostanziale delega alla macchina e al suo algoritmo della prova della propria responsabilità o della propria innocenza; dall'altro, poiché l'esito del test risulta ancorato allo studio dei tempi di reazione tra domanda e risposta, ossia alla diversa velocità con cui determinate frasi vengono associate tra loro, tempi questi calcolati da un algoritmo di cui l'esaminando – e la sua difesa, la pubblica accusa e chi deve giudicare sconosce tutto, e che non può in alcun modo verificare o falsificare. Ta-

le valutazione dei tempi di risposta si inserisce a valle di una complessa procedura empirica che richiede al soggetto testato di destreggiarsi, compiendo, il più velocemente e accuratamente possibile, plurime associazioni tramite lo schiacciamento di vari tasti, con ciò minacciando di intaccare la normale attitudine della persona all'autocontrollo, disorientandola ed estenuandone la volontà al fine di ottenere risposte che si collocano totalmente al di fuori della sua sfera di governo.

Aggiungono i giudici di seconde cure di Brescia che, in un sistema ove tutta la disciplina sulle prove orali è incentrata sulla necessità che queste siano ricercate e acquisite al di fuori dell'imputato, laddove quest'ultimo ha facoltà di astenersi dal deporre e, entro certi limiti, ha diritto di difendersi addirittura mentendo, la prova della innocenza-responsabilità dell'imputato non può essere ricercata somministrando allo stesso un test che, recuperando ricordi "impliciti", in grado anche di superare una volontaria manipolata rappresentazione dei fatti – *self-presentation artifact* –, sarebbe in grado di attribuire inequivocabili significati ai tempi con i quali costui, premendo pulsanti come da indicazione del somministratore, ha abbinato tra loro le varie frasi proposte.

6.7. *Il processo che verrà*

La valutazione operata dalla Corte non convince e palesa quell'approccio di fermo respingimento di qualunque interferenza nell'ambito di valutazione della veridicità delle dichiarazioni rese all'interno del processo di cui si è fatto cenno nelle pagine precedenti.

Le argomentazioni formulate poggiano infatti su ciò che appare un errore di comprensione delle metodiche in questione. Come noto, gli artt. 64, comma 2, e 188 c.p.p., congiuntamente affermano che «non possono esser utilizzati, neppure con il consenso della persona interessata, metodi o tecniche idonee a influire sulla libertà di determinazione o ad alterare le capacità di ricordare e di valutare i fatti». Se non si dubita che tali principi sbarrino decisamente l'ingresso nel nostro ordinamento processuale a metodiche quali narcoanalisi, ipnosi, *lie detector*, sieri e/o macchina della verità, non appare condivisibile sostenere che anche le metodiche quale quella sopra descritta sottraggono all'imputato che si sottopone al test ogni forma di autocontrollo sulla propria libertà di autodeterminazione e sulla capacità di ricordare e valutare i fatti.

Come chiaramente affermato in sede giurisprudenziale per primo dal giudice di Cremona, le tecniche in questione nulla hanno a che vedere con gli antiquati tentativi di verificare la "sincerità" di un soggetto tramite *lie detectors* o poligrafi, strumenti che pretenderebbero di fondare la valutazione su grossolani sintomi

psico-fisici del periziando, ma al contrario perseguono unicamente lo scopo di identificare se un determinato ricordo legato a uno specifico episodio risulti "naturale" e corrispondente o meno a quello descritto nell'imputazione.

L'*autobiographical Implicit Association Test*, del quale si può senz'altro discettare quanto alla sua scientificità, non può in nessun caso essere considerato uno strumento volto, seppur indirettamente, alla compressione della libertà morale del soggetto che vi si sottopone.

Sembra di poter affermare come la Corte di appello non abbia dato giusto valore alla puntuale spiegazione fornita loro dal perito all'uopo nominato che invece aveva ben chiarito come il test sfrutti una peculiare modalità organizzativa del sistema nervoso, l'*effetto compatibilità*, per cui la risposta motoria a informazioni codificate (ad esempio le tracce mnestiche) che nella mente del soggetto sono associate tra loro è più veloce che nel caso di informazioni codificate che non sono associate tra loro. Nessuna coercizione si delinea da queste precisazioni. Il test a-IAT è infatti unicamente una tecnica capace di rivelare e recuperare le tracce mnestiche di ricordi autobiografici genuini, di eventi realmente vissuti, registrati ed immagazzinati nella memoria del soggetto. La circostanza che esso abbia la possibilità di bypassare una serie di potenziali filtri o *bias* che il soggetto può, in qualche modo, anche inconsapevolmente, mettere in atto quando racconta, non può essere considerata una forma di coercizione.

Cosa diversa è invece rilevare come il suo miglior utilizzo sia stato individuato dal più volte evocato giudice di Cremona in considerazione del fatto che, la posizione dell'imputato, con il connesso diritto a mentire per difendersi, rende inevitabilmente meno credibile, meno utile, meno determinante, la sua dichiarazione processuale. Opportunamente aveva proceduto quel giudice a somministrare il test alla querelante, così come maggiormente utile potrebbe risultare il suo utilizzo rispetto alle dichiarazioni rese da un testimone. In tutti i casi, la prova di natura scientifica offerta al giudice attraverso la somministrazione del test in parola può risultare di una qualche utilità se posta a supporto e riscontro di altre prove acquisite, rafforzandone così la loro valenza.

Insomma, nella vicenda processuale di Cremona, l'a-IAT è stato più correttamente utilizzato come strumento accessorio, nel contesto di una valutazione psichiatrica più ampia, tendente a valutare il danno psichico della persona offesa.

Sebbene quindi l'utilizzo del test nei riguardi dell'imputato risulta meno convincente, non coglie nel segno la Corte d'appello di Brescia nell'affermare che esso miri a verificare se l'imputato dica o no la verità, ovvero se ha o meno commesso il delitto. Se così fosse non ci sarebbe dubbio alcuno che ci troveremmo di fronte un *lie detector* in piena regola; attrezzo che se trovasse cittadinanza nel processo con la connotazione di essere scientificamente "valido", ci troveremmo al cospetto di una rivoluzione epocale in grado di evitare,

finalmente, l'errore giudiziario, consentendo di raggiungere l'agognata certezza di condannare solo colpevoli.

Uno strumento di questo tipo non esiste. La contraddizione in cui incorre la Corte d'appello è tuttavia quella di accreditare prima il test in questione come scientificamente valido per poi lasciarlo fuori dal processo. Se quello che affermano i giudici di seconde cure di Brescia rispetto allo a-IAT fosse vero, per mera coerenza ogni procuratore generale presso ciascuna Corte di appello dovrebbe promuovere giudizio di revisione in tutti i casi in cui il ritenuto responsabile si sia dichiarato estraneo e si sia sottoposto con successo al test.

Altro rilievo sull'operato della Corte lo si rinviene, francamente, nella scelta di dare mandato in bianco a un esperto per la verifica sulla scientificità del test. Più corretto ovvero maggiormente responsabilizzante, sarebbe stata la scelta di provare a sciogliere la riserva confrontando direttamente la tecnica in questione con una griglia di valutazione, magari suggerita da un consulente, che potesse misurare la tecnica con degli "indici di scientificità", ovvero la lista *Daubert*, come operato ancora una volta dal più volte citato GIP di Cremona [39].

Occorre precisare che non si vuole formulare in questa sede un'obiezione nei riguardi del ricorso, di per sé, ad un esperto in ausilio, ma si ritiene che al perito sarebbe stato assai più opportuno rivolgere la richiesta di fornire elementi di conoscenza non appartenenti al cosiddetto *wealth of knowledge* del giudice e in grado di porre quest'ultimo nelle condizioni di decidere. Nel caso di specie, invece, si è optato per far decidere al perito al posto del giudice ed è questo aspetto a sollevare una forte perplessità, in considerazione, fra l'altro, che non può

[39] Concorda sul punto G. GENNARI, nota a sentenza App. Brescia, 15 luglio 2020 (dep. 11 novembre 2020), n. 1683, Pres. Deantoni, rel. Milesi, in *Sistema penale*, 2022, in cui pure l'Autore si esprime con vigore contro l'utilizzo del test in parola. Egli inoltre sottolinea come pur volendo identificare qualcuno al quale chiedere di rivedere gli studi che il consulente ha portato a sostegno della sua teoria, occorrerebbe che il processo di revisione fosse affidato a chi ha delle competenze specifiche in questa particolare e fondamentale attività di verifica del sapere scientifico; competenze che, quantomeno, richiedono una solida formazione statistica mentre nel caso di specie, la Corte ha affidato la perizia ad una neuro scienziata sicuramente di altissimo livello, ma che ha un curriculum essenzialmente da ricercatrice. La Corte sceglie un perito che ha un "peso" scientifico probabilmente non inferiore a quello del consulente, ma che non ha una competenza specifica nel settore di ricerca del consulente e che non ha un approccio meta-analitico. Questa scelta "intuizionistica" denota una scarsa per non dire nulla conoscenza dei processi che presiedono l'attività di revisione sistematica. L'Autore, ancora, mette in risalto come l'elaborato peritale non sembra potere essere qualificato come rassegna sistematica e, tantomeno, meta-analisi e ciò in considerazione del fatto che la lettura della perizia consente di notare che la gran parte della letteratura citata a sostegno della validità dell'a-IAT proviene dallo stesso Sartori o da suoi coautori. Questo potenziale "conflitto di interessi" avrebbe dovuto suggerire l'estrapolazione dei dati relativi agli studi sperimentali citati e la loro autonoma valutazione, cosa che invece non è stata fatta.

considerarsi scontato che il grado di certezza che consente di valutare "attendibile" un certo dato in ambito scientifico sia lo stesso che viene richiesto perché quello stesso dato sia utilizzabile in ambito giuridico [40].

Non di meno, ma questa obiezione non è per ovvie ragioni rivolta alla sentenza, viene da chiedersi se davvero le tecniche neuroscientifiche violino la libertà morale della persona e se per questo debbano essere vietate. Non è purtroppo questa la sede per sviluppare una riflessione sul punto ma chi scrive non può dirsi affatto certo che un innocente debba rimanere in carcere perché la prova che lo può liberare viola la sua libertà morale. Al contrario, a volerla dire tutta, si è piuttosto certi del contrario [41].

Senza cedere alla tentazione di alimentare nuovi miti o, se si preferisce, distruggerne vecchi, tenendo sempre in debito conto i rischi per la sicurezza e la tutela dei diritti fondamentali, quando trattiamo di Intelligenza Artificiale non dobbiamo mai tralasciare un elemento incontrovertibile ovvero che i dati sono la spina dorsale delle nuove tecnologie. Le tecnologie che consentono alle macchine di prendere decisioni in forma autonoma – "*machine learning*" e "*deep learnig*" – si basano nel primo caso su dati strutturati, un addestratore umano, un database controllabile, e un algoritmo variabile, mentre nel secondo caso su dati non strutturati, un sistema di autoapprendimento, un insieme di basi di dati molto vasto e una rete neurale di algoritmi. Sono sistemi molto potenti con margine di maturazione abbastanza ampi. Un fatto è però certo: se al sistema viene fornita sin dall'inizio una base di dati in entrata errata, la scelta e le decisioni conseguenti all'elaborazione di tali dati non potrà che essere sbagliata.

Garbage in, garbage out: se immetti spazzatura, alla fine del processo non avrai altro che spazzatura. Ecco, non si deve fare l'errore di temere queste nuove tecnologie ma neanche al contrario si devono demonizzarle.

Non bisogna sentirsi minacciati e, soprattutto in ambito processuale, non bisogna dimenticare che l'uomo, nel caso di specie il giudice, resta il soggetto deputato alla valutazione finale prodromica al pronunciamento della sentenza. Se l'a-IAT è da considerarsi una scienza buona, come affermato dal perito nominato dalla Corte d'appello di Brescia, patente che, al contrario, chi scrive non è certamente in grado di conferire, allora il suo utilizzo processuale non può esse-

[40] D'altronde sulla tecnica di formulazione dei quesiti peritali – notoriamente annosa questione – bisognerebbe aprire una lunga parentesi, osserva ancora G. GENNARI, nota a sentenza App. Brescia, 15 luglio 2020 (dep. 11 novembre 2020), n. 1683, Pres. Deantoni, rel. Milesi, cit.

[41] In termini molto analoghi, G. GENNARI, nota a sentenza App. Brescia, 15 luglio 2020 (dep. 11 novembre 2020), n. 1683, Pres. Deantoni, rel. Milesi, cit., il quale a sua volta chiama in causa questo tema A. BONOMI, *Libertà morale e accertamenti neuroscientifici: profili costituzionali*, in *BioLaw Journal – Rivista di BioDiritto*, 3, 2017.

re precluso, meno che meno perché essa viene intesa per ciò che non è; altresì la metodologia in questione non può certo diventare dominante all'interno del processo, come nessuna prova deve, se è vero come è vero che neanche la confessione dell'imputato "obbliga" il giudice a condannarlo.

Finché il principio del libero convincimento continuerà a lasciare al giudice la scelta finale circa la valutazione sulla colpevolezza dell'imputato, nessun automatismo potrà trovare ingresso nel processo penale e ciò dovrebbe rassicurare definitivamente tutti coloro che temono che un test sulla memoria autobiografica possa togliergli lo scettro della scelta finale sulla limitazione della libertà personale di un cittadino.

In definitiva, dobbiamo puntare sulle opportunità di sviluppo tecnologico orientato allo sviluppo di algoritmi di Intelligenza Artificiale anche all'interno del processo, purché essi siano ovviamente consolidati e riconosciuti dalla comunità scientifica di riferimento, ben consci delle problematiche che tale affermazione reca con sé.

CAPITOLO VII

Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini

MARCO COLACURCI

SOMMARIO: 7.1. Introduzione: i rischi della diffusione delle tecnologie di riconoscimento facciale da un'angolazione penalistica. – 7.2. Le TRF espressione del capitalismo della sorveglianza e della società del controllo. – 7.3. Il funzionamento delle TRF: datificazione e classificazione degli individui. – 7.4. I rapporti tra Stato e imprese nell'utilizzo delle TRF. L'esempio cinese: il ruolo ausiliario nella persecuzione della popolazione degli Uiguri. – 7.5. L'esempio statunitense: il ruolo "attivo" delle *big tech* e l'accusa di contribuire al razzismo endemico della polizia locale. – 7.6. Uno sguardo all'Italia: le pronunce del Garante per la *privacy* nei casi SARI e *Clearview AI*. – 7.7. Prime indicazioni dalla Proposta di Regolamento della Commissione europea e qualche considerazione conclusiva.

7.1. *Introduzione: i rischi della diffusione delle tecnologie di riconoscimento facciale da un'angolazione penalistica*

Nel marzo del 2022, con l'invasione dell'Ucraina da parte della Russia già in corso da alcune settimane, sui giornali è stata diffusa la notizia dell'arresto di un'attivista russa all'uscita dalla metropolitana di Mosca, qualche settimana dopo aver rilanciato su *Twitter* una manifestazione contro la guerra organizzata in piazza Pushkinskaya. L'attivista sarebbe stata identificata grazie al sistema di riconoscimento facciale *Sphere*, installato sui mezzi pubblici della capitale russa [1].

Quasi negli stessi giorni, ancora più risalto è stato dato alla notizia che la società *Clearview AI* si sia offerta di aiutare il governo ucraino mettendo a dispo-

[1] L. CARRER, *La Russia usa il riconoscimento facciale su chi manifesta contro la guerra*, 16 marzo 2022, in *www.wired.it*.

sizione i propri servizi per individuare infiltrati russi, riunire i rifugiati con le proprie famiglie e identificare le persone morte durante la guerra [2]. *Clearview AI* è una *startup* newyorchese che vende a imprese e agenzie di controllo pubbliche servizi di riconoscimento facciale basati su algoritmi allenati al riconoscimento a partire da un *database* di oltre dieci miliardi di immagini raccolte dai *social network* senza consenso delle persone interessate [3]. Le modalità di raccolta delle immagini e i servizi connessi, che sembrano permettere una profilazione e sorveglianza delle persone, hanno portato alcuni Stati a ritenere l'attività di *Clearview AI* contraria alla legge. Tra questi, come si avrà modo di vedere, c'è anche l'Italia [4].

Pochi mesi prima di questi eventi, *Apple* ha annunciato di aver migliorato il sistema di riconoscimento facciale installato sui modelli più recenti di *iphone*, permettendo di sbloccare il telefono con il proprio volto anche nel momento in cui si indossi una mascherina, a condizione che gli occhi siano ben visibili [5].

I tre esempi qui brevemente riportati consentono già di intuire in cosa consistano le Tecnologie di riconoscimento facciale (TRF) e quali applicazione possano ricevere: si tratta di sistemi in grado di identificare o autenticare una persona a partire dalle caratteristiche del volto [6]. Si è quindi nel campo della raccolta di dati biometrici, che permettono di distinguere le persone in base a particolari attributi del corpo quali, ad esempio, le impronte digitali, la forma dell'iride o il DNA [7]. Nel caso delle TRF, tuttavia, il dato da ottenere e analizzare è parti-

[2] K. CARBONI, *La più controversa startup di riconoscimento facciale sta collaborando con l'Ucraina*, 14 marzo 2022, in *www.wired.it*.

[3] L. ZORLONI, *Ho scoperto che la più discussa società di riconoscimento facciale al mondo ha le mie foto*, 23 marzo 2021, in *www.wired.it*.

[4] V. per ora il comunicato stampa del GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Riconoscimento facciale: il Garante privacy sanziona Clearview AI per 20 milioni di euro. Vietato l'uso dei dati biometrici e il monitoraggio degli italiani*, 9 marzo 2022, in *www.garanteprivacy.it*. Più ampiamente, *infra*, par. 5.

[5] *Ora è possibile sbloccare gli iPhone anche indossando la mascherina*, 15 marzo 2022, in *www.ilpost.it*.

[6] Nella dottrina giuridica interna, un lavoro monografico dedicato al tema è quello di G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale Scientifica, Napoli, 2021; v. anche, da un'angolazione processual-penalistica, E. SACCHETTO, Face to face*: il complesso rapporto tra* automated facial recognition technology *e processo penale*, in *www.lalegislazionepenale.it*, 16 ottobre 2020. Per una ricognizione della materia da una prospettiva penalistica, con specifico riguardo al contesto statunitense, cfr. New York City Bar, *Power, Pervasiveness and Potential: the Brave New World of Facial Recognition Through a Criminal Law Lens (and beyond)*, agosto 2020, in *http://documents.nycbar.org.s3.amazonaws.com/files/2020662-BiometricsWhitePaper.pdf*.

[7] L'art. 4, n. 14) del Regolamento generale sulla protezione dei dati (GDPR) definisce i

colarmente visibile e piuttosto facile da "raccogliere", sia nello spazio fisico sia in quello digitale [8].

Se, dal primo punto di vista, la messa a punto di tecnologie sempre più sofisticate punta a riconoscere un volto anche laddove sia parzialmente travisato, ad esempio con una mascherina, è nello spazio *online* che è possibile rinvenire, in maniera estremamente semplice, milioni quando non miliardi di immagini che ritraggono volti. Si pensi appunto ai *social network*, dove sono gli stessi utenti a caricare, volontariamente, le proprie foto, il più delle volte provvedendo anche a *taggarle* ossia a indicare a chi corrisponda un determinato volto, così contribuendo all'identificazione delle persone raffigurate.

Le TRF si presentano, dunque, come uno strumento dalle potenzialità applicative particolarmente ampie, sia dal punto di vista della diffusione potenzialmente capillare di strumenti di videosorveglianza diretti a "catturare" il volto delle persone sia delle numerose finalità a cui le stesse possono essere indirizzate, tanto di gestione della pubblica sicurezza quanto di natura prettamente commerciale [9]. Esse determinano un salto evolutivo significativo nella raccolta e gestione del dato biometrico, che lo rende suscettibile di molteplici utilizzi, come già risulta dagli esempi prima riportati, e che spaziano dall'impiego da parte della pubblica autorità per fini di controllo e sorveglianza oppure in contesti financo bellici alla messa in atto di strategie commerciali per aumentare la vendita di prodotti.

La natura anfibia di questi strumenti costituisce, dunque, un primo elemento degno di riflessione, che permette di illuminare il ruolo centrale giocato dalle imprese private nello sviluppo di tali tecnologie e nella vendita successiva alle amministrazioni governative e agenzie di controllo.

Infatti, si registra un apparente disallineamento tra la crescente diffusione delle TRF nell'ambito commerciale e alcune battute d'arresto rintracciabili nel campo della gestione della sicurezza pubblica, dove, negli ultimi tempi, alcu-

dati biometrici come «*i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici*». Essi rientrano, dunque, nell'elenco delle particolari categorie di dati di cui all'art. 9 del medesimo Regolamento, il cui trattamento è pertanto sottoposto a un regime di maggior tutela, con la possibilità, espressamente prevista dal medesimo art. 9, per ciascuno Stato di prevedere ulteriori restrizioni a simili trattamenti proprio allorquando si tratti di dati biometrici.

[8] Cfr. I. BERLE, *Face Recognition Technology. Compulsory Visibility and Its Impact on Privacy and the Confidentiality of Personal Identifiable Images*, Springer, Cham, 2020, *passim*.

[9] Per una ricognizione delle distinte finalità per cui possono essere utilizzate le TRF, v. T. HUANG, Z. XIONG, Z. ZHANGE, *Face Recognition Applications*, in S.Z. LI, A.K. JAIN (a cura di), *The Handbook of Face Recognition*, Springer, Cham, 2005, p. 617 ss.

ne tra le più grandi *tech company* hanno in parte smesso di fornire i propri prodotti alle forze dell'ordine per scopi di gestione dell'ordine pubblico. Questi comportamenti, visibili soprattutto nel contesto statunitense, non derivano da un'intervenuta disciplina di settore volta a restringerne il campo applicativo, ma sono conseguenza di precise scelte di *business*, motivate dalla volontà d'impresa di dissociarsi da pratiche oggetto di forti critiche da parte dell'opinione pubblica. Non a caso, si tratta di un *trend* che riguarda principalmente gli attori più importanti attivi sul mercato, ma che non sembra coinvolgere, invece, le imprese più piccole [10]. Ad ogni modo, si è in presenza di un fenomeno che fornisce un punto di vista parzialmente inedito nell'analisi dei rapporti tra impresa e Stato, con la prima a richiedere al secondo un intervento legislativo in un settore caratterizzato da uno squilibrio delle conoscenze in tutto favore dei soggetti privati [11].

Al contempo, il tema delle TRF sollecita un approfondimento dal punto di vista penalistico, non soltanto in relazione ai rischi di violazione del diritto alla *privacy* e al corretto trattamento dei dati personali, ma anche, e soprattutto, in ragione della possibilità di attuare, dietro ragioni di tutela della pubblica sicurezza, forme di sorveglianza [12] di massa e di profilazione [13] delle persone, con una severa compressione dei diritti fondamentali e costituzionalmente garantiti della personalità nonché di riunione, associazione e libera manifestazione del pensiero [14]. A tal riguardo, da più parti si è messo in luce come l'installazione di

[10] *Infra*, par. 4.

[11] Su come lo squilibrio di conoscenze in settori a elevata complessità tecnologica favorisca il diffondersi di fenomeni auto-normazione (più o meno regolata) d'impresa cfr. soprattutto G. FORTI, *Principio di precauzione e diritto penale*, in *Criminalia*, 2006, p. 196 ss., nonché C. PIERGALLINI, *Danno da prodotto e responsabilità penale*. *Profili dommatici e politico-criminali*, Giuffrè, Milano, 2004, p. 301 ss. Sul fenomeno dell'autonormazione, all'interno di una vasta bibliografia, v. da ultimo D. BIANCHI, *Autonormazione e diritto penale. Intersezioni, potenzialità, criticità*, Giappichelli, Torino, 2021.

[12] Da intendersi come la «*raccolta ed elaborazione di dati personali, identificabili o meno, allo scopo di influenzare o controllare coloro ai quali essi appartengono*»: così, D. LYON, *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, Feltrinelli, Milano, 2002, p. 2. V. anche G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Raffaello Cortina Editore, Milano, 2015.

[13] Ai sensi dell'art. 4 del GPDR, per profilazione s'intende «*qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica*».

[14] G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., p. 57 ss.

TRF in spazi pubblici possa esplicare effetti di auto-censura da parte della popolazione, scoraggiata dall'esercitare tali fondamentali diritti (*chilling effect*) [15].

Dunque, l'idea di un potere pubblico in grado di esercitare un controllo pervasivo e costante delle persone, che consenta di tenere traccia del comportamento di ciascuno a partire dalle riprese effettuate dai sempre più diffusi sistemi di videosorveglianza, non sembra rappresentare la concretizzazione di un immaginario distopico o riconducibile alla sola realtà di Stati autoritari. Certamente, in ordinamenti in cui vi è un minore rispetto delle libertà personali, alcuni usi delle TRF spingono verso l'ulteriore compressione di diritti fondamentali: oltre all'esempio già fatto della Russia, si vedrà come in Cina il riconoscimento facciale contribuisca a perpetrare quello che è stato definito come il genocidio culturale della popolazione degli Uiguri, minoranza musulmana e turcofona che vive nel nord-ovest del paese [16].

Nondimeno, è opportuno inquadrare i rischi ingenerati dall'uso (e abuso) di simili tecnologie anche alle nostre latitudini, dove, ad esempio, le forze di polizia dispongono di un sistema di riconoscimento facciale la cui funzione "*real time*" – fino ad oggi non ancora utilizzata – è stata di recente ritenuta illegittima dal Garante per la protezione dei dati personali perché priva di un'adeguata base legale. Al riguardo, il Garante ha appunto stigmatizzato i rischi derivanti da una simile tecnologia, capace di attuare delle vere e proprie forme di sorveglianza di massa [17]. Non a caso, nelle più recenti proposte di regolamentazione della materia elaborate a livello di Unione europea, le TRF sono incluse tra i sistemi di intelligenza artificiale ad alto rischio, il cui utilizzo va adeguatamente limitato o, in alcuni casi, addirittura bandito [18].

La particolare cautela con cui affrontare il tema deriva dalla capacità di queste tecnologie di ridisegnare il rapporto tra potere statuale e cittadini, tra autorità e libertà: un mutamento che passa anche da una nuova e diversa concezione dello spazio pubblico, inteso come luogo in cui ognuno è visibile e di conseguenza tracciabile. Spazio pubblico "fisico" che funge, a ben vedere, da specchio rove-

[15] Sul cd. *chilling effect*, tra i contributi più recenti, v. F. VIGANÒ, *La proporzionalità della pena. Profili di diritto penale e costituzionale*, Giappichelli, Torino, 2021, p. 277 ss.; N. RECCHIA, *Il principio di proporzionalità nel diritto penale*, Giappichelli, Torino, 2020, p. 252 ss.

[16] V., ad es., M. CLARKE, *Framing the Xinjiang emergency: colonialism and settler colonialism as pathways to cultural genocide?*, in ID. (a cura di), *The Xinjiang emergency Exploring the causes and consequences of China's mass detention of Uyghurs*, Manchester, 2022, p. 10 ss. Più ampiamente, *infra* par. 4.

[17] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sul sistema SARI real time*, 25 marzo 2021. Più in dettaglio, *infra*, par. 5.

[18] *Infra*, par. 6.

sciato del mondo *online*, dove è ancora più facile divenire oggetti di uno stretto monitoraggio, così rinsaldando il legame che avvince dimensione pubblica e privata dell'utilizzo delle TRF.

In quest'ottica, prima di procedere a un'analisi ravvicinata del fenomeno, appare opportuno compiere un passo indietro, per tentare di inquadrare la diffusione del riconoscimento facciale all'interno della società contemporanea.

7.2. *Le TRF espressione del capitalismo della sorveglianza e della società del controllo*

Profilazione, controllo e sorveglianza costituiscono elementi caratteristici delle società attuali, rispetto alle quali la proliferazione delle TRF, supportato dal comportamento aggressivo di imprese dai fatturati paragonabili o superiori a quelli degli Stati più evoluti, sembra porsi in maniera perfettamente coerente. Come illustrato nel lavoro già classico di Shoshana Zuboff, l'ultima evoluzione del modello socio-politico del capitalismo avrebbe riconfigurato l'attività d'impresa in un senso "estrattivo" ossia rivolto in via prioritaria ad acquisire dati sul comportamento delle persone, per poi utilizzarli per scopi commerciali [19]. Non si tratta soltanto della possibilità di fare previsioni su gusti e comportamenti di un certo *target*, ma anche di sfruttare i dati a disposizione per incidere, mediante meccanismi di condizionamento, sul comportamento effettivo delle persone, da orientare nel senso ritenuto più vantaggioso da un punto di vista economico [20].

La possibilità per le imprese di attingere a una mole vastissima di dati deriva dalla crescente digitalizzazione delle attività umane, favorita dalla diffusione di sistemi, a partire dagli *smartphone*, che consentono di individuare una "traccia" di ciò che si è compiuto. D'altronde, in letteratura si è efficacemente proposto di definire con il termine *onlife* la dimensione soltanto all'apparenza scissa che l'uomo contemporaneo vive, diviso tra la vita *online* e quella *offline*, che appunto si ritiene non possano più continuare a essere considerate in maniera separata [21].

Ebbene, gli effetti del capitalismo della sorveglianza non s'impongono soltanto nella strutturazione delle attività economiche, ma incidono in profondità anche nell'assetto delle relazioni sociali. Le potenzialità del controllo pervasivo a cui chiunque può essere sottoposto determinano, infatti, un mutamento nei

[19] Cfr. S. ZUBOFF, *The age of surveillance capitalism. The Fight for a Human Future at the New Frontier of Power*, Public Affairs, New York, 2019.

[20] ID., spec. p. 65 ss.

[21] La felice espressione è stata coniata da L. FLORIDI, *The Onlife Manifesto. Being Human in a Hyperconnected Era*, Springer, Cham, 2015.

comportamenti quotidiani, all'interno di quello che viene definito come un nuovo *panopticon* digitale, un sistema di controllo che opererebbe come una sorta di super-io collettivo in grado di condizionare "da remoto" i comportamenti individuali e indirizzarli in vista di una loro monetizzazione [22].

D'altronde, in letteratura si è segnalato come le metafore prese in prestito dall'immaginario distopico da "Grande fratello", solitamente adoperate per descrivere società connotate da una massiccia sorveglianza dei cittadini, risultino inadeguate a descrivere quella che, in altre e precedenti teorizzazioni, è stata inquadrata come società del controllo [23], quale forma che avrebbe sostituito le precedenti società disciplinari, entrate irrimediabilmente in crisi nel corso del Novecento [24].

Queste ultime erano caratterizzate dalla presenza di istituzioni per così dire "rigide", all'interno delle quali l'individuo era anzitutto contenuto fisicamente e quindi disciplinato, lungo un arco temporale potenzialmente capace di coprire una vita intera (famiglia scuola caserma fabbrica ospedale) [25]. Nella società del controllo si assiste, invece, a una rarefazione e contestuale moltiplicazione degli strumenti – appunto – di controllo: «*i controlli sono una modulazione, come una modellatura auto-deformante, che si modifica continuamente, da un istante all'altro, o come un setaccio le cui maglie cambiano da un punto all'altro*» [26]. In un tale contesto, a occupare il campo non è più la fabbrica, ma l'impresa, che gestisce salari, premi e promozioni mediante meccanismi che stimolano la competitività tra le persone [27].

[22] S. ZUBOFF, *The age of surveillance capitalism*, cit., p. 438, dove l'A. descrive la nuova realtà in cui gli individui sono immersi: «*a new phenomenon to live continuously in the milieu of the gaze of others, to be followed by hundreds or thousands of eyes, augmented by Big Other's devices, sensors, beams, and waves rendering, recording, analyzing, and actuating*».

[23] G. DELEUZE, *Les sociétés de contrôle* (1990), ora disponibile in *EcoRev'*, 1, 2018, p. 5 ss.

[24] Così, D. LYON, *La cultura della sorveglianza. Perché la società del controllo ci ha reso tutti controllori*, Luiss University Press, Roma, 2020, p. 19 ss. V. anche G. BALBI, P. DI SALVO, *Introduzione all'edizione italiana. La sorveglianza: un tema "classico" per capire il contemporaneo*, ivi, p. 9 ss.

[25] Sulle società disciplinari, imprescindibile il riferimento a M. FOCAULT, *Sorvegliare e punire. Nascita della prigione* (1975), Einaudi, Torino, 2014. Nella letteratura interna, altrettanto obbligatorio il rimando a M. PAVARINI, D. MELOSSI, *Carcere e fabbrica. Alle origini del sistema penitenziario* (1977), Il Mulino, Bologna, 2018. Sulla (successiva) perdita di centralità dell'istituzione carceraria e sull'esercizio di un controllo latamente penale all'interno e da parte dell'intera collettività, altrettanto doveroso è il riferimento a D. GARLAND, *La cultura del controllo. Crimine e ordine sociale nel mondo contemporaneo* (2001), Il Saggiatore, Milano, 2004.

[26] G. DELEUZE, *Les sociétés de contrôle*, cit., p. 7.

[27] *Ibidem*.

Proprio la constatazione del carattere maggiormente orizzontale del controllo, differente dalla "verticalità" con cui è esercitato il potere disciplinare, è valorizzata da chi pone in relazione l'affermarsi della società del controllo con il diffondersi di una cultura della sorveglianza generata dagli stessi utenti [28]. Al riguardo, sia sufficiente riprendere l'esempio dei *social network*, e della mole di informazioni che da essi possono essere ricavate, semplicemente "seguendo" una persona nella sua vita *online* [29].

Si ribalta, dunque, l'idea che concepisce un sorvegliante munito di poteri particolarmente penetranti e una moltitudine di sorvegliati: in un contesto iper-connesso, sono le stesse persone suscettibili di controllo a rendersi, a loro volta, solerti controllori. Da questa angolazione, la collettività è immersa all'interno di una vera e propria cultura della sorveglianza. Accanto a quella tradizionale, messa in campo, in maniera più o meno legittima, da agenzie di *intelligence*, governi e poteri digitali, si pone il comportamento dei singoli cittadini, che erige una simile attività a pratica quotidiana.

I concetti di capitalismo della sorveglianza, società del controllo e cultura della sorveglianza, ancorché diretti a inquadrare da angolazioni parzialmente diverse l'evoluzione degli assetti socio-economici delle società contemporanee, convergono, quindi, nel delineare uno scenario in cui la costante tracciabilità delle vite umane consente l'immagazzinamento di dati e al contempo diffonde forme di sorveglianza orizzontali [30]. La possibilità di ricorrere a tecnologie di riconoscimento facciale, che come tali consentono di identificare e tracciare le persone a partire dal proprio volto, si inserisce in maniera perfettamente congruente in un simile scenario, imprimendo una particolare curvatura alle pratiche estrattive tipiche del capitalismo della sorveglianza [31]. In questo campo, infatti, persino il volto umano è ridotto a un insieme di dati, da disaggregare e utilizzare per le finalità più disparate.

Per comprendere meglio questo elemento, è dunque opportuno esaminare con maggior grado di dettaglio al funzionamento di tali tecnologie.

[28] D. LYON, *La cultura della sorveglianza*, cit., p. 25 ss.

[29] Per un catalogo delle «*pratiche della sorveglianza*», ivi, p. 59 ss.

[30] V. le considerazioni sviluppate ivi, p. 50 ss.

[31] Diversi esempi connessi all'utilizzo delle TRF sono illustrati già da S. ZUBOFF, *The age of surveillance capitalism*, cit., spec. p. 230 ss., all'interno del paragrafo dedicato all'estrapolazione dei dati direttamente dal corpo (*body rendition*).

7.3. *Il funzionamento delle TRF: datificazione e classificazione degli individui*

In via di prima approssimazione, le TRF compiono un trattamento in modo automatizzato di immagini digitali che contengono il volto di una persona: ricorrendo a tecniche biometriche, ne sono ricavati i caratteri identificativi, riportati in forma di codici alfanumerici ed eventualmente arricchiti da indici ulteriori (*hashing*) [32].

Tale processo può essere utilizzato per finalità di autenticazione/verifica della persona, mediante l'abbinamento del volto dal vivo alla foto – ad esempio – presente su un documento di identità, di identificazione, tramite l'individuazione di una corrispondenza (*match*) tra la fotografia e quelle già raccolte e contenute in un *database*, e, infine, di rilevazione ossia di individuazione dei volti a partire, ad esempio, da telecamere a circuito chiuso, da confrontare con le foto presenti in un *database* alla ricerca di una corrispondenza.

Le TRF permettono che la ricerca del *match*, indicato per il tramite di un indice percentuale, avvenga in maniera particolarmente rapida e in relazione a centinaia di migliaia di foto. Questa potrà essere realizzata sia in modalità "da remoto" sia "in tempo reale": nel primo caso, si tratta appunto di ricercare una corrispondenza tra l'immagine acquisita e quelle già presenti nel *database*; nel secondo, le TRF permetteranno di operare un confronto tra una moltitudine di volti, "catturati" in tempo reale, e quelli già presenti a catalogo. Ad esempio, si potrebbe ricorrere a tale tecnica per individuare un soggetto ritenuto pericoloso all'interno di una folla facendo ricorso a videocamere di sorveglianza puntate su aree pubbliche.

È tale ultima modalità a destare le maggiori perplessità, in quanto comporta, in linea potenziale, una sorveglianza di massa, in assenza di qualunque forma di consenso da parte delle persone oggetto del trattamento. Nel prosieguo si vedrà come le proposte di regolamentazione mirino a limitare fortemente la possibilità di ricorrere a tali forme di riconoscimento facciale, privilegiandosi quelle che operano *ex post* [33].

Ad ogni modo, in tutti i casi è operata una categorizzazione delle persone, a prescindere dall'identità delle stesse, semplicemente isolando le caratteristiche tipiche del volto del soggetto ritratto [34]. Tale operazione è realizzata grazie al

[32] Illustra in dettaglio il funzionamento delle TRF, G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., p. 32 ss. V. anche J. BUOLAMWIN, V. ORDÓÑEZ, J. MORGENSTERN, E. LEARNED-MILLER, *Facial recognition technologies: a primer*, Algorithmic Justice League, 29 maggio 2020, disponibile in *https://people.cs.umass.edu/~elm/papers/FRTprimer.pdf*.

[33] *Infra*, parr. 5 e 6.

[34] La cd. «*indifferenza formale*» verso gli utenti caratterizza, a ben vedere, il capitalismo

ricorso a strumenti di apprendimento automatico, tipici di sistemi che vengono definiti di intelligenza artificiale. Il riconoscimento facciale pertiene, quindi, a un sotto-campo dell'IA, quello della visione artificiale, che si occupa appunto di insegnare alle macchine a rilevare e interpretare le immagini. Come segnalato in letteratura, si tratta di un ambito particolarmente problematico, stante la natura relazionale e spesso inafferrabile delle immagini [35].

Pertanto, al fine di istruire la macchina alla comprensione di ciò che "vede", si parte dalla raccolta di un campione quanto più esteso possibile di immagini, opportunamente catalogate ed etichettate. Come noto, nel vasto settore del cd. *deep learning*, il processo di apprendimento e miglioramento continuo delle macchine avviene mediante delle tecniche di correlazione induttiva e inferenza probabilistica basate sulla frequenza statistica con cui si replicano determinati schemi nel campione. Non vi è, dunque, un'effettiva comprensione degli stessi, quanto, appunto, un progressivo raffinamento delle capacità di individuare correlazioni interne a ciò che viene processato [36].

Così, nel campo delle TRF, una volta che alla macchina sono state presentate le immagini entra in gioco un algoritmo (*learner*) che guida l'apprendimento a partire dai dati etichettati e che, a sua volta, informa un ulteriore algoritmo (*classifier*) sulle modalità con cui individuare le relazioni tra i nuovi *input* e gli *output* attesi. Il miglioramento costante di un simile sistema è dunque strettamente dipendente dalla mole dei dati analizzati e dal grado di precisione con cui sono stati etichettati. Una volta messi a punto *set* di dati stabilizzati per lo sviluppo della visione artificiale, questi fungono da base di partenza per il perfezionamento dei diversi sistemi, a seconda degli obiettivi di volta in volta prefissati [37].

I sistemi di riconoscimento facciale necessitano, allora, di poter attingere a un catalogo quanto più ampio e variegato possibile di immagini, capace di alimentare e istruire macchine voraci e all'apparenza insaziabili. Da ciò ne discende, da un canto, la raccolta "selvaggia" del materiale disponibile in rete, compiuta nell'assenza sostanziale del consenso da parte delle persone coinvolte, e, dall'altro, il ricorso a *database* già esistenti e concepiti per altri utilizzi, come ad esempio accaduto con le raccolte di foto segnaletiche a disposizione delle autorità di pubblica sicurezza. Ne discendono problematiche connesse non soltanto

della sorveglianza in sé e le pratiche che gli sono tipiche: cfr. S. ZUBOFF, *The age of surveillance capitalism*, cit., p. 353 ss.

[35] K. CRAWFORD, *Né intelligente né artificiale. Il lato oscuro dell'IA*, Il Mulino, Bologna, 2021, p. 119 ss.

[36] V. ad es. S. QUINTARELLI (a cura di), *Intelligenza artificiale. Cos'è davvero, come funziona, che effetti avrà*, Bollati Boringhieri, Milano, 2020; M. CHIRIATTI, *Incoscienza artificiale. Come fanno le macchine a prevedere per noi*, Luiss University Press, Roma, 2021.

[37] K. CRAWFORD, *Né intelligente né artificiale*, cit., p. 111 ss.

al rispetto del diritto alla *privacy* delle persone le cui foto sono state utilizzate per allenare i sistemi di riconoscimento facciale, ma anche in termini di affidabilità dei sistemi, dipendenti dalla varietà dei dati e dalla correttezza dell'etichettamento [38].

A tal riguardo, da più parti si sono evidenziati i *racial bias* dei sistemi di riconoscimento facciale, meno allenati a riconoscere persone di determinati generi o colori della pelle [39], e, di volta in volta, le aziende coinvolte hanno cercato di rimediare ampliando la tipologia di dati a cui fanno ricorso [40]. Nondimeno, in letteratura si è criticato questo *modus operandi*, diretto a correggere problematiche ritenute al contrario insite nei sistemi di intelligenza artificiale e discendenti in maniera diretta dall'attività di classificazione che è alla base del processo di apprendimento delle macchine: «*Le pratiche di classificazione danno forma al modo in cui l'intelligenza artificiale viene classificata e prodotta* (…) *tutto ciò che esiste al mondo viene convertito in dati attraverso l'estrazione, la misurazione, l'etichettatura e l'ordinamento, e questo diventa, intenzionalmente o meno, una scivolosa evidenza empirica per i sistemi tecnologici addestrati su questi dati*» [41].

Ne risulta che le TRF sembrano realizzare al massimo grado il processo di "datificazione" dell'individuo, ridotto a mero dato numerico; al medesimo tempo, si contribuisce alla costruzione di generi e razze in base alle quali distinguere artificialmente il genere umano. In letteratura si sollecita dunque a interrogarsi su chi compia una siffatta catalogazione e su quali basi [42]: una questione che diviene ancora più pressante allorché si pretenda di classificare le persone a partire dalle caratteristiche del proprio volto e che chiama in causa le imprese private impegnate nello sviluppo dei sistemi di intelligenza artificiale.

[38] Ivi, spec. p. 141 ss.

[39] Cfr., ad es., I. IVANOVA, *Why face-recognition technology has a bias problem*, in *www.cbsnews.com*, 12 giugno 2020; A. NAJIBI, *Racial Discrimination in Face Recognition Technology*, in *https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/*, 24 ottobre 2020. V. anche *Coded Bias*, documentario del 2020 che indaga, appunto, i pregiudizi e le discriminazioni realizzate dagli algoritmi, in particolar modo nei sistemi di riconoscimento facciale.

[40] V., ad es., J. ROACH, *Microsoft improves facial recognition technology to perform well across all skin tones, genders*, 26 giugno 2018, articolo apparso sul sito della società *Microsoft*, nonché R. PURI, *Mitigating Bias in AI Models*, 6 febbraio 2018, articolo apparso sul sito della società *IBM*.

[41] K. CRAWFORD, *Né intelligente né artificiale*, cit., p. 144.

[42] Ivi, p. 164 ss.

7.4. *I rapporti tra Stato e imprese nell'utilizzo delle TRF. L'esempio cinese: il ruolo ausiliario nella persecuzione della popolazione degli Uiguri*

Una volta osservata la non neutralità alla base del funzionamento delle TRF, e più in generale dei sistemi di IA, strettamente dipendente dalle modalità di classificazione dei dati a partire dai quali le macchine "imparano", ai fini delle presenti riflessioni appare opportuno concentrarsi, altresì, sul ruolo – anfibio e ambiguo – occupato dall'impresa nella diffusione di tali strumenti presso le forze di pubblica sicurezza [43].

Un ruolo che muta, evidentemente, al variare del contesto osservato, a seconda della natura più meno autoritaria dello Stato di riferimento, ma che in ogni caso conferma come le *big tech* di fatto forniscano la tecnologia necessaria a forme di sorveglianza di massa, quando non sono esse stesse a promuovere il ricorso a simili strumenti, soprattutto laddove si muovano in ambiti scarsamente disciplinati e al riparo dall'attenzione mediatica. Al contrario, qualora esigenze reputazionali lo suggeriscano, sono le medesime imprese a prendere le distanze dagli utilizzi controversi delle TRF, in alcuni casi anche mediante l'interruzione dei rapporti commerciali con Stati e agenzie federali.

La Cina sembra offrire un chiaro esempio di brutale utilizzo dell'IA e delle TRF per scopi di sorveglianza e profilazione di massa. Se l'ambizione a divenire *leader* mondiale nel settore ha determinato una diffusione di queste tecnologie all'interno di città sempre più connesse e "*smart*", nella regione dello Xinjiang, dove risiede la popolazione degli Uiguri, sembra si stia compiendo un vero e proprio esperimento totalitario [44].

Agli strumenti tradizionali di controllo sociale si affiancano, infatti, quelli più tecnologici, al fine di ottenere una sorveglianza a tappeto e permanente di tale minoranza etnico-religiosa, giustificata dal governo cinese per ragioni di contrasto al terrorismo. La raccolta dei dati degli Uiguri è associata all'elaborazione di modelli predittivi – rischio criminale compreso – rivelando in manie-

[43] Così D. LYON, *La cultura della sorveglianza*, cit., p. 50: «*La sorveglianza è anche una grande industria. Le* corporation *globali vi prendono parte e spesso hanno stretti legami con il governo*».

[44] Cfr. S. PIERANNI, *Red Mirror. Il nostro futuro si scrive in Cina*, Laterza, Roma, 2020, p. 52 ss. Ma v. anche le risoluzioni del Parlamento europeo del 17 dicembre 2020 sul lavoro forzato e la situazione degli uiguri nella regione autonoma uigura dello Xinjiang, del 19 dicembre 2019 sulla situazione degli uiguri in Cina ("*China Cables*"), del 18 aprile 2019 sulla Cina, in particolare la situazione delle minoranze religiose ed etniche, e del 4 ottobre 2018 sulla detenzione di massa arbitraria di uiguri e kazaki nella regione autonoma uigura dello Xinjiang.

ra plastica come l'installazione di telecamere e la diffusione di *app* di controllo sociale si presti a declinazioni liberticide nei rapporti tra autorità e cittadini. Le nuove tecnologie, incluse quelle di riconoscimento facciale, sono utilizzate nell'ambito di una politica di "rieducazione" promossa dal partito comunista e che comprende anche forme di detenzione di massa [45].

I tentativi di portare all'attenzione della Corte Penale Internazionale tali pratiche, così da avviare un'indagine, non sono andati a buon fine: nel dicembre 2021, l'Ufficio del Procuratore ha ritenuto che non vi fossero le basi giuridiche per procedere per genocidio e crimini di guerra, in quanto i fatti sarebbero avvenuti prevalentemente nel territorio della Repubblica popolare cinese, che non ha ancora aderito allo Statuto di Roma [46].

Invece, si è assistito al proliferare di sanzioni di natura economica, promosse in primo luogo dagli Stati Uniti e indirizzate anche verso le imprese multinazionali cinesi accusate di contribuire alle pratiche di individuazione e confinamento della popolazione uigura. In particolare, i primi *ban* sono stati emanati durante il mandato presidenziale di Donald Trump, inserendosi all'interno di una più generale politica di accesa competizione commerciale con la Cina [47]. Nondimeno, anche nel corso della presidenza di Joe Biden si è proseguito lungo la medesima direttrice, e lo scorso dicembre è stato approvato il cd. *Uyghur Forced Labor Prevention Act*, che prevede, tra le altre cose, il divieto di importazione dei prodotti dalla regione dello Xinjiang, a meno che le imprese non dimostrino, in maniera "chiara" e "convincente" di essere estranee a pratiche di sfruttamento del lavoro [48].

Inoltre, sempre nel dicembre 2021, alcune imprese cinesi, accusate di contribuire alla sorveglianza biometrica e al tracciamento della popolazione uigura, sono state inserite in una delle *blacklist* messe a punto dell'*Office of Foreign*

[45] Si legga il recente *report* di HUMAN RIGHTS WATCH, *"Break Their Lineage, Break Their Roots". China's Crimes against Humanity Targeting Uyghurs and Other Turkic Muslims*, 19 aprile 2021, disponibile in *www.hrw.org/report/2021/04/19/break-their-lineage-break-their-roots/chinas-crimes-against-humanity-targeting#_ftn109*.

[46] G. PANE, *Il popolo abbandonato degli Uiguri: il Prosecutor della CPI chiude le indagini contro la Cina*, in *www.iusinitinere.it*, 28 settembre 2021. Per il comunicato della Corte, v. THE OFFICE OF THE PROSECUTOR, INTERNATIONAL CRIMINAL COURT, *Report on Preliminary Examination Activities 2020*, 14 dicembre 2020, par. 70 ss., in *www.icc-cpi.int/sites /default/files/itemsDocuments/2020-PE/2020-pe-report-eng.pdf*.

[47] Cfr. A. NISSEN, *Import Bans on Products from Forced Labor in the Trump Era*, in *Un. Bologna L. Rev.*, 2020, p. 367 ss.

[48] Per una ricognizione a prima lettura, v., ad es., GIBSON DUNN, *The Uyghur Forced Labor Prevention Act Goes Into Effect in the United States*, 14 gennaio 2022, in *www.gibsondunn.com/the-uyghur-forced-labor-prevention-act-goes-into-effect-in-the-united-states/*.

Assets Control (OFAC) presso il Dipartimento del Tesoro statunitense. La competenza di tale ufficio si radica a partire dalla valuta usata nelle transazioni, il dollaro, e ad essa di riconnette il potere di vietare rapporti commerciali in dollari con Stati, individui e gruppi di persone ritenuti una minaccia alla sicurezza, alla politica estera o all'economia nazionale [49].

Anche l'Unione europea ha reagito: sulla base della Decisione 2020/1999 del Consiglio del 7 dicembre 2020, sono state applicate misure restrittive a quattro alti ufficiali cinesi nella regione dello Xinjiang per le violazioni dei diritti umani sulla minoranza musulmana degli uiguri [50].

Oltre alle sanzioni economiche, è opportuno prendere in considerazione anche l'effetto reputazionale delle accuse mosse alle imprese di essere coinvolte in tali pratiche: una vasta eco mediatica hanno avuto le notizie che riguardavano società cinesi come *Alibaba* e *Huawei*, "giganti" del settore: la prima, tra le più importanti multinazionali nel campo dell'*e-commerce*, è stata accusata di aver messo a punto un *software* in grado, a partire da filmati o fotografie caricati dagli utenti, di individuare e segnalare persone appartenenti alla minoranza uigura [51]. La seconda, attiva nel settore delle telecomunicazioni e già destinataria di una serie di *ban* dovuti ad accuse di spionaggio, si ritiene fornisca alla polizia cinese un sistema di *scan* facciale capace di individuare una persona di etnia uigura e, eventualmente, di inviare un *alert* [52]. In entrambi i casi, le aziende si sono difese dichiarando che si tratta di sistemi soltanto testati in via di prova e non destinati ad utilizzi che possano contribuire a pratiche discriminatorie e dannose per i diritti umani [53].

[49] Dal sito dell'OFAC: *https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20211216*. Sul tema, v., ad es., V. ORTBLAD, *Criminal Prosecution in Sheep's Clothing: The Punitive Effects of OFAC Freezing Sanctions*, in 98 *J. Crim. L. and Criminology*, 2008, p. 1439 ss. Nella letteratura interna, particolare attenzione all'attività dell'OFAC, anche in relazione alle regole di *compliance* d'impresa, è prestata da S. MANACORDA, *The "Dilemma" of Criminal Compliance for Multinational Enterprises in a Fragmented Legal World*, in S. MANACORDA, F. CENTONZE (a cura di), *Corporate Compliance on a Global Scale. Legitimacy and Effectiveness*, Springer, Cham, 2022, p. 67 ss.

[50] Cfr. *Council implementing Regulation (EU) 2021/478 of 22 March 2021 implementing Regulation (EU) 2020/1998 concerning restrictive measures against serious human rights violations and abuses*, disponibile in *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2021:099I:FULL&from=EN*.

[51] H. DAVIDSON, *Alibaba offered clients facial recognition to identify Uighur people, report reveals*, 20 dicembre 2020, in *www.theguardian.com*.

[52] V. NI, *Documents link Huawei to Uyghur surveillance projects, report claims*, 15 dicembre 2021, in *www.theguardian.com*.

[53] V. *Statement from Alibaba Group Regarding Recent Reports of the Company's Facial Recognition Technology*, 16 dicembre 2020, in *www.alizila.com/statement-from-alibaba-gro*

In un contesto autoritario come quello cinese, dunque, sembrano trovare attuazione particolari modelli di sorveglianza totale, con le imprese attive nel settore che rivestono un ruolo ausiliare, consistente nella messa a disposizione di tecnologie idonee alla realizzazione di simili politiche. Al medesimo tempo, l'utilizzo di tali tecnologie su scala così vasta ne contribuisce al miglioramento, atteso che, come già osservato, quanto maggiore è la mole di dati processati dai sistemi di IA tanto più rapida e precisa ne sarà l'evoluzione [54].

7.5. *L'esempio statunitense: il ruolo "attivo" delle* big tech *e l'accusa di contribuire al razzismo endemico della polizia locale*

Nel volgere lo sguardo, invece, a una democrazia liberale come quella statunitense, il ruolo delle imprese nel contribuire alla diffusione di strumenti di controllo e sorveglianza presso le forze di polizia appare maggiormente riconducibile all'incontro tra gli interessi commerciali delle prime e gli obiettivi di gestione dell'ordine pubblico delle seconde. In altre parole, nel vuoto normativo che caratterizza il settore, l'utilizzo o meno di simili strumenti sembra rimesso, in buona parte, alle scelte dei singoli uffici e alle eventuali sinergie che vengono a instaurarsi con le *corporation* che li producono.

Così, *Rekognition*, il sistema di riconoscimento facciale messo a punto da *Amazon*, è stato al centro di progetti-pilota sviluppati in alcune città, tra cui, ad esempio, Orlando [55]. In questo caso, il progetto è terminato in virtù del fatto che la città non disponesse della tecnologia adeguata al funzionamento del sistema in modalità *real time* [56]. Già prima dell'interruzione della sperimentazione, però, numerose associazioni di attivisti, ma anche impiegati e *shareholder* di *Amazon*, avevano protestato contro i rischi derivanti dal suo utilizzo, proteste rimaste tuttavia inascoltate dall'impresa [57].

up-regarding-recent-reports-of-the-companys-facial-recognition-technology/; le dichiarazioni da parte di Huawei sono riportate da E. DOU, *Documents link Huawei to China's surveillance programs*, 14 dicembre 2021, in *www.washingtonpost.com*.

[54] Lo sottolinea S. PIERANNI, *Red Mirror*, cit., p. 55.

[55] D. ALBA, *With No Laws To Guide It, Here's How Orlando Is Using Amazon's Facial Recognition Technology*, 30 ottobre 2018, in *www.buzzfeed.com*.

[56] N. STATT, *Orlando police once again ditch Amazon's facial recognition software*, 18 luglio 2019, in *www.theverge.com*.

[57] J. VINCENT, *AI researchers tell Amazon to stop selling "flawed" facial recognition to the police*, 3 aprile 2019, in *www.theverge.com*; ID., *Amazon employees protest sale of facial recognition software to police*, 22 giugno 2018, ivi; C. LECHER, *Shareholders are pushing Amazon to stop selling its facial recognition tool*, 17 gennaio 2019, ivi.

Soltanto qualche tempo dopo, invece, la società ha deciso di vietare, prima per un anno e poi anche per quello successivo, la vendita di *Rekognition* alle forze di polizia, anticipando di qualche mese le società *IBM* e *Microsoft*. Il deciso cambio di rotta da parte di *Amazon* e di altre tra le più importanti *tech company* al mondo è da ascriversi al moto di reazioni e proteste che in tutti gli Stati Uniti sono seguite falla morte di George Floyd, un uomo nero di 46 anni morto a causa della tecnica di immobilizzazione cd. *knee on neck* alla quale è stato sottoposto nel corso di un arresto da parte di Dereck Chauvin, un ufficiale di polizia bianco [58].

Nell'ambito delle critiche al razzismo strutturale che pervaderebbe la società statunitense e si rifletterebbe in maniera vistosa nelle attività degli apparati di polizia [59], alle *big tech* si è contestato di fornire strumenti di controllo e sorveglianza massiva, a loro volta viziati da *racial* (e *gender*) *bias*, con le TRF più allenate a identificare uomini bianchi. La necessità di prendere le distanze dalle attività della polizia ha dunque portato le multinazionali in questione a rivedere le proprie politiche aziendali in materia e a interrompere i contratti in essere, in attesa di una disciplina legislativa sul tema.

La soluzione più radicale è quella adottata da *IBM*: nel giugno 2020, il CEO ha dichiarato che la società non avrebbe più sviluppato, compiuto ricerche e venduto TRF per scopi di *law enforcement*. Al medesimo tempo, con una lettera indirizzata al Congresso degli Stati Uniti, ha sollecitato a disciplinare la materia, ponendo in risalto l'estrema opacità alla base dei rapporti tra le agenzie di controllo e le imprese impegnate nella vendita di tali tecnologie nonché, soprattutto, i rischi di «*mass surveillance, racial profiling, violations of basic human rights and freedoms*» [60]. *Microsoft*, invece, analogamente ad *Amazon*, ha temporaneamente interrotto le sue attività nei confronti degli organi dello Stato, in attesa di un'espressa disciplina del settore [61].

[58] R. CORNELLI, *Note sulla* Police brutality *a partire dai fatti di Minneapolis*, in *Riv. trim. dir. pen. cont.*, 2, 2020, p. 1 ss.

[59] Esalta il fattore razziale nelle pratiche violente della polizia statunitense, R. CORNELLI, *La forza di polizia. Uno studio criminologico sulla violenza*, Giappichelli, Torino, 2020, p. 25 ss. Mette in luce la natura sistematica dell'addestramento alla violenza a cui sono formati gli agenti di polizia negli Stati Uniti, E. GRANDE, *La condanna di Derek Chauvin per la morte di George Floyd: giustizia è fatta?*, 14 maggio 2021, in *www.questionegiustizia.it*.

[60] Il testo della lettera è disponibile in: *www.ibm.com/blogs/policy/facial-recognition-sunset-racial-justice-reforms/*.

[61] A. LEVY, *Microsoft says it won't sell facial recognition software to police until there's a national law "grounded in human rights"*, 11 giugno 2020, in *www.cnbc.com*; K. WEISE, N. SINGER, *Amazon Pauses Police Use of Its Facial Recognition Software*, 10 giugno 2020, in *www.nytimes.com*.

Le scelte delle *corporation* di interrompere la fornitura di sistemi di riconoscimento facciale appaiono quindi dettate, almeno in primo luogo, da esigenze reputazionali [62]. In una fase storica connotata da profonde tensioni e divisioni in senso alla società statunitense, i rischi per i colossi tecnologici di essere percepiti dai consumatori come fornitori di sistemi in grado di perpetuare forme di discriminazione e razzismo da parte degli agenti di polizia è stato considerato evidentemente troppo alto. In tal senso, il comune richiamo a una regolamentazione pubblica della materia è espressione evidente della necessità di poter aderire a un insieme codificato di regole a cui attenersi, di modo da poter agire nella legalità e, soprattutto, di poter dichiarare di farlo. Sebbene già fossero noti i pericoli discendenti dall'utilizzo delle TRF, è stata l'esplosione della questione razziale a rivelarsi determinante nello spingere le imprese a rimeditare le proprie scelte di *business*.

Negli Stati Uniti, all'iniziale opacità nella diffusione del riconoscimento facciale tra forze di polizia è quindi seguita una fase di sovraesposizione mediatica che ha inquadrato criticamente la questione, spingendo i *competitor* più in vista a uscire dal mercato. Tutto ciò, tuttavia, non ha ancora portato a una regolamentazione a livello federale. Così, permane il rischio che, a fronte della scelta delle maggiori società di dissociarsi da pratiche commerciali malviste dai consumatori, siano aziende più piccole ad occupare il campo e soddisfare la domanda [63].

7.6. *Uno sguardo all'Italia: le pronunce del Garante per la* privacy *nei casi SARI e* Clearview AI

Nel contesto italiano, o meglio europeo, sebbene allo stato non via sia ancora una regolamentazione in materia di riconoscimento facciale, deve registrarsi un crescente interesse per la questione. Ne è significativo testimone la Risoluzione del Parlamento europeo del 6 ottobre 2021 sull'uso dell'IA nel diritto penale, in cui, tra le altre cose, si chiede alla Commissione «*una moratoria sulla diffusione dei sistemi di riconoscimento facciale per le attività di contrasto con funzione di identificazione*» [64], in attesa della garanzia che tali tecnologie siano con-

[62] Sull'importanza della dimensione reputazionale nell'esercizio dell'attività d'impresa, e sui costi derivanti da una "*bad reputation*", v. il numero speciale della rivista *Buss.&Soc.*, 6, 2019, intitolato appunto *Corporate Reputation: Being Good and Looking Good*, e in particolare D. BREITINGER, J.P. BONARDI, *Firms, Breach of Norms, and Reputation Damage*, p. 1143 ss.

[63] J. HOROWITZ, *Tech companies are still helping police scan your face*, 3 luglio 2020, in *www.edition.cnn.com*.

[64] *Risoluzione del Parlamento europeo del 6 ottobre 2021 sull'intelligenza artificiale nel*

formi ai diritti fondamentali e immuni da pregiudizi discriminatori, e vi sia un quadro giuridico tale da evitarne un uso distorto e improprio. Nel medesimo testo, si esprime profonda preoccupazione «*per l'utilizzo di database privati di riconoscimento facciale da parte delle autorità di contrasto e dei servizi di intelligence, come* Clearview AI*, una banca dati di oltre tre miliardi di immagini raccolte illegalmente dai social network e da altre fonti Internet*» [65].

A seguito di tale Risoluzione, l'Italia ha effettivamente approvato una moratoria dei sistemi biometrici di riconoscimento facciale in luoghi pubblici o aperti al pubblico fino alla fine del 2023, ad eccezione, tuttavia, dei trattamenti effettuati dalle autorità competenti a fini di prevenzione e repressione dei reati, o anche di esecuzione di sanzioni penali ai sensi del d.lgs. n. 51/2018. Una soluzione temporanea, in attesa dell'approvazione del Regolamento sulla cd. legge sull'intelligenza artificiale [66].

Si delinea, quindi, uno scenario in rapido mutamento, in cui la recente attenzione di legislatore e opinione pubblica costituisce un elemento di novità. A differenza degli Stati Uniti, infatti, dove l'assenza di leggi federali favorisce l'attività di imprese multinazionali nell'incidere e direzionare le scelte dell'autorità nelle modalità di gestione di ordine e sicurezza pubblici, grazie anche a dei programmi pilota con cui testare e migliorare tali strumenti, nello scenario europeo si registra una maggiore volontà di regolamentare la materia. Ciononostante, vi sono casi significativi di utilizzo delle TRF tutt'altro che scevri da problematiche.

Guardando all'Italia, sin dal 2017 il Ministero dell'Interno dispone del *Sistema automatico di riconoscimento immagini* (SARI). Quest'ultimo, ad oggi, è utilizzato nella sola funzione da remoto, denominata *Enterprise*, che consente l'identificazione di un soggetto ignoto a partire da un'immagine fotografica. In particolare, mediante «*una ricerca computerizzata nella banca dati AFIS, e grazie a due algoritmi di riconoscimento facciale,* [SARI Enterprise] *è in grado di fornire un elenco di immagini ordinato secondo un grado di similarità*» [67]. A sua volta, la banca dati AFIS (*Automated Fingerprint Identification System*) rappresenta il sistema automatizzato di acquisizione delle impronte digitali, di cui fa parte il *Sotto sistema anagrafico* (SSA), che contiene, invece, le foto segnaleti-

diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale (2020/2016(INI)), par. 27.

[65] Ivi, par. 28.

[66] V. artt. da 9 a 12, l. n. 3374/2021, di conversione del d.l. n. 139/2021.

[67] Così si può leggere sul sito del Ministero dell'Interno, *www.interno.gov.it*. Sul tema, in letteratura, v. R. LOPEZ, *La rappresentazione facciale tramite* software, in A. SCALFATI (a cura di), *Le indagini atipiche*, Giappichelli, Torino, 2019, p. 239 ss.

che presenti nei *database* della polizia, insieme alle informazioni fisiche delle persone ritratte.

SARI *Enterprise* è venuto alla pubblica ribalta nel settembre 2018, quando il suo utilizzo ha consentito l'identificazione e l'arresto di due persone di origine georgiana accusate di aver compiuto un furto in un'abitazione qualche mese prima: grazie alle immagini riprese dalle videocamere di sorveglianza, il sistema ha potuto individuare una corrispondenza tra i milioni di immagini presenti nel *database* [68]. In tale occasione, la Polizia di Stato ha comunicato che la fase di sperimentazione era terminata e che SARI rappresentava un importante ausilio nel contrasto alla criminalità [69].

Se, dunque, in precedenza era necessario immettere manualmente i tratti caratterizzanti il volto della persona ricercata per sperare di ottenere dal sistema qualche corrispondenza, con SARI questa operazione è automatizzata. Proprio perché rappresenta una semplice sofisticazione nel trattamento delle immagini, appena qualche mese prima dell'identificazione delle persone accusate di furto in abitazione il Garante per la protezione dei dati personali aveva dato il via libera a SARI *Enterprise*. Nel relativo provvedimento si era osservato, infatti, che tale funzione rappresenta «*un mero ausilio all'agire umano, avente lo scopo di velocizzare l'identificazione, da parte dell'operatore di polizia, di un soggetto ricercato della cui immagine facciale si disponga, ferma restando l'esigenza dell'intervento dell'operatore per verificare l'attendibilità dei risultati prodotti dal sistema automatizzato*» [70].

Diametralmente opposta è stata, invece, la decisione del medesimo Garante sulla modalità *real time* di SARI, intervenuta soltanto di recente, a causa, come svelato da un'inchiesta giornalistica, delle resistenze opposte dal Ministero dell'Interno alla richiesta di fornire una valutazione d'impatto sulla *privacy* dei cittadini (DPIA), come noto necessaria allorché il trattamento possa comportare un rischio elevato per i diritti e le libertà delle persone interessate [71]. L'istruttoria, aperta nel 2017, è arrivata soltanto nel 2021 a conclusione. Nel frattempo, il Ministero dell'Interno aveva pubblicato un bando per potenziare ulteriormente

[68] V., ad es., *Brescia: ladri d'appartamento identificati con il riconoscimento facciale*, 7 settembre 2018, in *www.repubblica.it*.

[69] *Ecco Sari, il nuovo software di riconoscimento facciale della polizia*, 7 settembre 2018, in *www.skytg24.it*.

[70] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Sistema automatico di ricerca dell'identità di un volto*, provvedimento n. 440 del 26 luglio 2018.

[71] R. COLUCCINI, *Lo scontro Viminale-Garante sul riconoscimento facciale*, in *IRPImedia*, 13 gennaio 2020, disponibile in *https://drive.google.com/file/d/1oGPsVzM-TH6JQu0hNX7F8VsLBAIN-7bE/view*.

la funzione *real time* di SARI, in modo da utilizzarlo come «*sistema tattico per monitorare le operazioni di sbarco e tutte le varie tipologie di attività illegali correlate, video riprenderle ed identificare i soggetti coinvolti*» [72]: nuovamente, il riconoscimento facciale sembra indirizzarsi a detrimento di particolari face deboli della popolazione, in questo caso le persone migranti [73].

Come accennato, tuttavia, nel marzo 2021 il Garante ha espresso parere non favorevole all'utilizzo di SARI *real time*, in quanto non sussiste una base legale adeguata per tale attività. La pronuncia in questione illustra chiaramente i rischi derivanti dal ricorso a forme di riconoscimento facciale in tempo reale, che «*realizza un trattamento automatizzato su larga scala che può riguardare, tra l'altro, anche coloro che siano presenti a manifestazioni politiche e sociali, che non sono oggetto di "attenzione" da parte delle forze di Polizia*» [74], potendo determinare «*una evoluzione della natura stessa dell'attività di sorveglianza, passando dalla sorveglianza mirata di alcuni individui alla possibilità di sorveglianza universale allo scopo di identificare alcuni individui*» [75].

A fondamento della propria decisione, il Garante pone la constatazione che quelli oggetto di trattamento rappresentano categorie particolari di dati ai sensi dell'art. 9 RGPD, in quanto «*dati biometrici intesi a identificare in modo univoco una persona fisica*» [76], nonché, in virtù del potenziale utilizzo nell'ambito di manifestazioni pubbliche, di dati idonei a rivelare le opinioni politiche o l'appartenenza sindacale. Pertanto, il loro trattamento è sottoposto alle condizioni più stringenti dettate dall'art. 7 d.lgs. n. 51/2018, tra cui quella di dovere essere «*specificamente previsto dal diritto dell'Unione europea o da legge o, nei casi previsti dalla legge, da regolamento*» [77].

Al riguardo, è interessante sottolineare come il Garante non consideri una base legale adeguata il decreto di attuazione del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per finalità di

[72] Ivi, p. 2.

[73] V. il report di HERMES, CENTRO PER LA TRASPARENZA E I DIRITTI UMANI DIGITALI, *Tecnologie per il controllo delle frontiere in Italia. Identificazione, riconoscimento facciale e finanziamenti europei*, 2020, disponibile in *https://s3.documentcloud.org/documents/21128523/tecnologie-per-il-controllo-delle-frontiere-in-italia-identificazione-riconoscimento-facciale-e-finanziamenti-europei.pdf*.

[74] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sul sistema Sari Real Time*, provvedimento n. 127 del 25 marzo 202.

[75] *Ibidem*. Per un commento ai provvedimenti del Garante, cfr. anche G. MOBILIO, *Tecnologie di riconoscimento facciale*, cit., p. 240 ss.

[76] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sul sistema Sari Real Time*, cit., par. 2) delle osservazioni.

[77] *Ibidem*.

polizia, da organi, uffici e comandi di polizia. Sebbene sia qui prevista una specifica disciplina per il trattamento dei dati raccolti mediante sistemi di videosorveglianza e di ripresa fotografica, audio e video, a parere del Garante si tratta di «*sistemi ontologicamente diversi da quelli dei dati biometrici*» [78].

Infine, come accennato in apertura di lavoro, il Garante per la protezione dei dati personali si è anche occupato di *Clearview AI*, società che offre alle autorità pubbliche un servizio di ricerca e trattamento mediante TRF delle immagini sul *web* liberamente accessibili. Il procedimento, nato a seguito di notizie stampa che denunciavano le criticità nella gestione dei dati da parte di *Clearview AI*, e a quattro reclami di persone che avevano scoperto che la società deteneva diverse immagini che le raffiguravano senza che avessero prestato consenso, ha fatto chiarezza sull'attività svolta, ritenendola in contrasto con le disposizioni del GDPR relative ai principi che devono caratterizzare il trattamento dei dati (di correttezza e trasparenza, di limitazione delle finalità e di limitazione della conservazione), alle condizioni di liceità del trattamento in generale e a quelle previste per particolari tipologie di dati sensibili, nonché con riguardo al rispetto dei diritti dell'interessato. Pertanto, è stata ordinata l'applicazione della sanzione amministrativa pecuniaria nel limite edittale massimo di venti milioni di euro [79].

La decisione del Garante si rivela di particolare interesse perché illustra in modo plastico le pratiche di sorveglianza e profilazione permesse dalle TRF a partire dal materiale accessibile *online*. Mediante tecniche di *web scraping* – normalmente vietate dai gestori dei siti, in particolare di *social network* – la società raccoglie foto pubblicamente accessibili da siti o da video disponibili in rete, per poi elaborarle con tecniche biometriche. Una volta indicizzate, queste possono essere arricchite con i metadati disponibili associati all'immagine (ad es. la pagina *web* da cui è stata presa, la data di nascita della persona ritratta, la nazionalità, la lingua parlata etc.), che saranno trasmesse una volta trovata la corrispondenza.

Da tutto ciò il Garante ne ricava che l'attività svolta non consiste, come dichiarato dalla Società, nella mera classificazione di individui sulla base di caratteristiche note, ma nella gestione di dati biometrici che consente un tracciamento nel tempo delle persone ad essi associate [80].

[78] *Ibidem*.

[79] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Ordinanza ingiunzione nei confronti di* Clearview AI, provvedimento n. 50 del 10 febbraio 2022.

[80] *Ibidem*: «*Le informazioni in questione formano oggetto di archiviazione nel database di* Clearview *e vengono arricchite nel tempo con altre estratte da nuovi* template *idonei a riflettere anche i cambiamenti fisici avuti dallo stesso soggetto, come emerge dall'esame di alcuni dei reclami proposti all'Autorità* (…). *Ne discende che* Clearview *non offre come ri-*

7.7. *Prime indicazioni dalla Proposta di Regolamento della Commissione europea e qualche considerazione conclusiva*

La ricognizione compiuta sinora ha mostrato come il campo delle TRF sia stato interessato, nel corso degli ultimi anni, da un dibattito sempre più ampio, dove stanno trovando spazio e riconoscimento le voci più critiche e preoccupate circa la diffusione di tali strumenti per finalità di gestione della pubblica sicurezza, specialmente in assenza di una disciplina che regoli chiaramente la materia. Nel caso specifico dell'Italia, le pronunce del Garante per la protezione dei dati personali hanno censurato alcune forme di utilizzo delle TRF capaci di aprire la strada a forme di sorveglianza di massa e profilazione nel tempo delle persone, ribadendo con forza la necessità di una legge sul tema. Il Parlamento italiano ha approvato una moratoria sulla possibilità di usare sistemi di videosorveglianza dotati di riconoscimento facciale in luoghi pubblici – sebbene con l'eccezione, tra le altre, dell'ipotesi in cui il trattamento sia effettuato dalle autorità competenti a fini di prevenzione e repressione dei reati – in ciò allineandosi all'indicazione contenuta nella Risoluzione del Parlamento europeo sulla richiesta alla Commissione di bandire tali tecnologie, quantomeno in attesa di un intervento legislativo che ne assicuri l'uso in maniera compatibile al rispetto dei diritti fondamentali.

Al riguardo, sono rinvenibili diversi esempi di linee guida, ove le condizioni per l'utilizzo del riconoscimento facciale sono più o meno stringenti anche a seconda dell'organismo che le ha elaborate[81]. Al contempo, alcune iniziative promosse da associazioni a tutela dei diritti digitali e fondamentali delle persone mirano a sensibilizzare l'opinione pubblica affinché siffatte tecnologie vengano

sultato della ricerca una semplice corrispondenza, ma anche un archivio di risorse che si snoda attraverso il tempo. La valutazione di tale circostanza, unitamente alla finalità comparativa sopra evidenziata, è idonea ad integrare, come richiesto nel Considerando 24, un'attività assimilabile al controllo del comportamento dell'interessato in quanto posta in essere tramite il tracciamento in internet e la successiva profilazione».

[81] Ad es., se nel documento elaborato dal UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS, *Report. The right to privacy in the digital age*, 13 settembre 2021, par. 45, si condivide la proposta già avanzata dal Parlamento europeo di una moratoria sull'uso di quei sistemi in grado di compromettere diritti fondamentali, come accade con il riconoscimento facciale, almeno fino a quando non sia provato che tali rischi siano stati neutralizzati, il recente *white paper* intitolato *A Policy Framework for Responsible Limits on Facial Recognitio Use Case: Law Enforcement Investigations* e messo a punto nell'ambito del *World Economic Forum* con la partecipazione di Interpol e UNICRI, contiene significative aperture all'utilizzo delle TRF. Particolarmente rilevanti, altresì, sono le linee guida elaborate dal COMITATO CONSULTIVO 108 istituito presso il Consiglio d'Europa, dal titolo *Guidelines on Facial Recognition*, del 28 gennaio 2021.

messe al bando [82]. Le motivazioni sono molteplici e spaziano dall'inaffidabilità alla circostanza per cui i costi, in termini di compressione dei diritti e di mutamento nella relazione tra autorità e libertà, sono di gran lunga maggiore dei benefici.

In un tale scenario, la proposta di Regolamento in materia di intelligenza artificiale [83], il primo tentativo compiuto nel contesto europeo di disciplinare in maniera organica l'IA, costituisce un parametro di riferimento particolarmente importante, anche alla luce dell'intensa attività preparatoria che lo ha preceduto, condensata in numerosi atti di impulso e strumenti di *soft law* [84]. Nell'ambizione di disciplinare l'utilizzo dell'IA mediante un «*approccio equilibrato*» [85], che sia consapevole che «*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*» [86], la proposta di Regolamento qualifica alcuni usi dell'IA come vietati o ad alto rischio, in questo secondo caso prevedendo delle particolari condizioni che siano in grado di attenuarlo [87].

Ebbene, il tema dell'identificazione biometrica riceve ampia considerazione, proprio in virtù dei potenziali rischi per i diritti fondamentali che ne possono discendere. Coerentemente alle modalità con cui tali sistemi possono operare, si distingue tra l'identificazione biometrica in tempo reale e da remoto: la prima,

[82] V. soprattutto la campagna "*Reclaim your face*", un'Iniziativa dei cittadini europei (ECI) – strumento di partecipazione diretta che consente di proporre alla Commissione europea l'approvazione di nuove leggi – con cui si chiede «*di vietare, nel diritto e nella pratica, gli usi indiscriminati o tendenziosi della biometria che possono sconfinare in attività di sorveglianza di massa illecita*». In Italia, la campagna è promossa dal Centro Hermes per la trasparenza e i diritti umani digitali.

[83] *Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza Artificiale*, 21 aprile 2021.

[84] V. ad es. le due risoluzioni del Parlamento europeo sui principi etici dell'IA, della robotica e della tecnologia correlata, nonché sul regime di responsabilità civile per l'IA, entrambi del 20 ottobre 2020, e la risoluzione sull'uso dell'IA del 20 gennaio 2021, nonché il Libro bianco sull'Intelligenza artificiale della Commissione, del 19 febbraio 2020. In dottrina, cfr. L. PARONA, *Prospettive europee e internazionali di regolazione dell'intelligenza artificiale tra principi etici,* soft law *e* self regulation, in *Riv. regolaz. mercati*, 1, 2020, p. 70 ss.

[85] *Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza Artificiale*, cit., Relazione, cap. 1, Contesto della proposta.

[86] *Ibidem*.

[87] Per una ricognizione del contenuto della proposta, cfr. C. CASONATO, B. MARCHETTI, *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, in *BioLaw J.*, 1, 2021, p. 1 ss.

in spazi pubblici e per attività di contrasto, è vietata in quanto ritenuta particolarmente invasiva dei diritti e delle libertà delle persone interessate «*nella misura in cui potrebbe avere ripercussioni sulla vita privata di un'ampia fetta della popolazione, farla sentire costantemente sotto sorveglianza e scoraggiare in maniera indiretta l'esercizio della libertà di riunione e di altri diritti fondamentali*» [88].

Nondimeno, si prevedono delle significative eccezioni a una simile messa al bando, allorché questi sistemi si rendano necessari per la ricerca di potenziali vittime di reato, compresi i minori scomparsi, la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone o di un attacco terroristico, nonché il rilevamento, la localizzazione, l'identificazione o l'azione penale nei confronti di un autore o di una persona sospettata di un reato per cui può essere spiccato un mandato d'arresto europeo, allorché tale reato sia punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno tre anni [89].

Anche qualora si versi in una delle descritte situazioni, ai fini del trattamento dei dati dovrà tenersi conto della natura della situazione che dà luogo al possibile uso, in particolare la gravità, la probabilità e l'entità del danno causato dal mancato uso del sistema, e le conseguenze dell'uso del sistema per i diritti e le libertà di tutte le persone interessate, in particolare la gravità, la probabilità e l'entità di tali conseguenze. L'uso dovrà essere subordinato a un provvedimento motivato dell'autorità giudiziaria o amministrativa dello Stato membro, ad eccezione dei casi in cui ragioni di urgenza non autorizzino a procedere immediatamente, rimandando la richiesta di autorizzazione a una fase successiva [90].

Invece, per quel che concerne i sistemi di identificazione biometrica da remoto, questi sono inquadrati tra i sistemi di IA ad alto rischio [91]. Concordemente, il loro utilizzo deve rispettare una serie di condizioni, tra cui l'attuazione, per tutto il ciclo di vita del sistema, di un meccanismo di *risk-management* volto a individuare e minimizzare i rischi prevedibili prima della messa in commercio o emersi durante l'utilizzo, a cui si accompagnano contestuali obblighi di informazione al pubblico e di *testing* costante dei sistemi, nonché il rispetto di stan-

[88] *Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza Artificiale*, cit., considerando n. 18). La disciplina è contenuta al Titolo II – Pratiche di Intelligenza Artificiale vietate, art. 5.

[89] *Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza Artificiale*, cit., Titolo II, art. 5, lett. d).

[90] *Ibidem*.

[91] Ivi, Allegato III – Sistemi di IA ad alto rischio di cui all'art. 6, par. 2.

dard qualitativi dei dati che fungono da base per l'addestramento dei sistemi ad alto rischio al fine di contenere errori e discriminazioni. Un aspetto, quest'ultimo, particolarmente rilevante in relazione alle tecnologie di riconoscimento facciale, come visto sovente affette da pregiudizi di genere o legati al colore della pelle delle persone [92]. Inoltre, si richiede che il sistema sia «*sufficientemente trasparente*», così da permettere di comprendere come funzioni il meccanismo di apprendimento della macchina, e che assicuri un'efficace supervisione umana. Infine, tali sistemi dovranno sottostare a una procedura di verifica di conformità a standard e regole stabilite dall'Unione, che potrà essere effettuata dal produttore stesso o da un organismo certificatore terzo [93].

Come si evince da questa pur rapida ricognizione della proposta di Regolamento, il tema del riconoscimento facciale, e più in generale dell'identificazione biometrica, è inquadrato in termini problematici, alla luce delle potenziali ricadute negative sui diritti fondamentali. Se nella modalità da remoto si prevede una serie di condizioni che consente di vigilare sul concreto utilizzo delle TRF e, di riflesso, sulle sue finalità, la consapevolezza circa la possibilità di realizzare forme di sorveglianza di massa attraverso la modalità in tempo reale spinge verso la scelta, ben più radicale, del divieto.

Nondimeno, è facile accorgersi come le eccezioni a siffatto divieto siano suscettibili di ricevere un'applicazione estensiva. Non solo l'elenco eterogeneo dei reati per i quali è prevista la possibilità di ricorrere a un mandato d'arresto europeo, ma il riferimento a situazioni di emergenza o di attacchi terroristici, da un canto, e alle attività di ricerca di vittime, compresi minori scomparsi, dall'altro, sembra inquadrare scenari emergenziali rispetto ai quali appare lecito ricorrere anche ai mezzi più controversi per conseguire lo scopo prefissato.

Visti da un'angolazione penalistica, le condizioni dettate dalla proposta per derogare al divieto riguardano ambiti e obiettivi politico-criminali – il contrasto al terrorismo specialmente, ma anche, in parte, la tutela delle vittime – che hanno legittimato profonde trasformazioni del diritto penale [94]. Nel caso delle TRF,

[92] *Supra*, par. 3.

[93] Ivi, Titolo III – Sistemi di IA ad alto rischio, artt. 8 ss. Per un commento delle condizioni richieste dalla Proposta per i sistemi di IA ad alto rischio, v. C. CASONATO, B. MARCHETTI, *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, cit., p. 13 ss.

[94] Si tratta di una bibliografia vastissima: v., ad es., M. DONINI, *Diritto penale di lotta vs. diritto penale del nemico*, in A. GAMBERINI, R. ORLANDI (a cura di), *Delitto politico e diritto penale del nemico*, Monduzzi, Bologna, 2007, p. 131 ss.; invece, sugli aspetti in chiaroscuro sul sistema di garanzie penalistiche discendenti dalla diffusione del cd. paradigma vittimario, cfr. tra i tanti C. ELIACHEFF, S. LARIVIÈRE, *Il tempo delle vittime. Come le vittime sono diventate i nuovi eroi della società democratica contemporanea* (2007), Ponte alle grazie, Firenze,

il richiamo a scenari emergenziali per giustificarne l'uso anche in *real time* ripropone nuovamente uno schema collaudato di rinuncia parziale a determinate garanzie per finalità di pubblica sicurezza [95].

Tuttavia, come si è osservato nel corso della presente trattazione, la diffusione di tali tecnologie in siffatte modalità rischia di trasformare in maniera irreversibile il rapporto tra potere e cittadini. Le ulteriori condizioni dettate dalla proposta, inerenti alla verifica della gravità della situazione e alla previa autorizzazione dell'autorità (nel caso in cui ragioni d'urgenza non consentano di richiederla in seguito) non sembrano poter contenere il rischio di città puntellate di telecamere di videosorveglianza munite di TRF, che seppure "silenti" – in quanto utilizzabili solo al verificarsi di un'emergenza – molto probabilmente eserciterebbero un effetto dissuasivo nell'esercizio di diritti fondamentali dei cittadini.

Come già accennato, alcune associazioni attive nel campo della tutela dei diritti fondamentali e dei diritti digitali si battono perché il riconoscimento facciale venga messo al bando, senza eccezioni. In questo senso va la recente proposta di emendamenti al Regolamento, presentata il 31 marzo 2022, che prevede, tra le altre cose, il divieto assoluto di ricorrere alle tecniche di identificazione biometrica in tempo reale [96].

In ogni caso, anche laddove il Regolamento sia approvato nell'attuale conformazione, ciascuno Stato membro sarà libero di limitare ulteriormente l'uso delle TRF [97]. A quel punto, sarà necessario un dibattito pubblico partecipato e consapevole, che metta in chiara luce rischi e benefici derivanti da tali tecnologie, e che sia dunque capace di orientare le scelte del legislatore.

2008, nonché, per un lavoro di taglio monografico, M. VENTUROLI, *La vittima nel sistema penale. Dall'oblio al protagonismo?*, Jovene, Napoli, 2015.

[95] V. il sempre attuale lavoro di S. MOCCIA, *La perenne emergenza. Tendenze autoritarie nel sistema penale*, II ed., ESI, Napoli, 2000.

[96] La proposta di emendamenti è disponibile in: *www.europarl.europa.eu/doceo/document/ITRE-AM-719802_IT.pdf*.

[97] *Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza Artificiale*, cit., art. 5, par. 4.

CAPITOLO VIII

L'utilizzo dell'intelligenza artificiale nel campo delle attività investigative delle forze dell'ordine: tra prospettive di sviluppo ed esigenze di coordinamento

CHIARA PISTILLI

SOMMARIO: 8.1. Premessa. – 8.2. L'intelligenza artificiale applicata alle attività di polizia. In particolare: il suo impiego nell'ambito delle tradizionali attività di indagine. – 8.3. I sistemi di intelligenza artificiale in uso al Raggruppamento Operativo Speciale dei Carabinieri. – 8.3.1. Lo strumento di analisi delle immagini. – 8.3.2. Lo strumento di analisi del testo ed elaborazione del linguaggio naturale. – 8.3.3. Lo strumento per analisi del parlato e *speech recognition*. – 8.4. Riflessioni conclusive.

8.1. *Premessa*

L'impatto dell'intelligenza artificiale sugli strumenti a disposizione delle forze dell'ordine è stato dirompente.

Questa vera e propria rivoluzione tecnologica quale può essere considerata l'intelligenza artificiale (nel prosieguo IA), in grado di simulare e riprodurre con straordinaria efficacia le funzioni cognitive e le operazioni proprie dell'intelletto umano, si è rivelata – nel bene e nel male – in grado di impattare notevolmente sulle nostre vite e sul complesso sociale e lavorativo in cui ciascuno di noi è costantemente calato.

Le operazioni cui l'uomo è fisiologicamente avvezzo – dalla comprensione del linguaggio al riconoscimento di oggetti e di suoni, fino all'apprendimento e alla risoluzione di problematiche di svariata portata e gravità – sono ora artificialmente eseguibili da una macchina per effetto dell'utilizzo di *software* di ultima generazione in grado di riprodurre meccanismi analoghi a quelli tipici dell'intelletto e del corpo. Un essere umano riconosce e percepisce intuitivamente determinate situazioni sviluppando gli *input* sensoriali che per natura gli appartengono e pone in essere le corrispondenti azioni al fine di reagire prontamente

ad essi; il suo cervello è in grado di assumere decisioni nell'immediatezza e di trasmetterle al corpo affinché lo stesso dia concretezza ai movimenti che di quelle decisioni costituiscono concreta estrinsecazione.

Tutto ciò è oggi possibile grazie all'IA, questo rivoluzionario meccanismo in costante evoluzione orientato a replicare su un elaboratore elettronico funzioni di pertinenza esclusiva dell'intelligenza umana che consente alle macchine artificiali di poter svolgere le azioni proprie dell'uomo, dal riconoscimento vocale e visivo fino all'assunzione di processi decisionali e predittivi.

Pur dando atto delle perduranti difficoltà insite nella individuazione di una definizione univoca, precisa e integrata di IA, allo stato mancante, essa è attualmente considerata un sistema dotato di un'elevata capacità logico-computazionale in grado di simulare il funzionamento del cervello umano e di prendere decisioni analizzando una grande quantità di dati e di informazioni elaborate [1].

Efficace, in tal senso, nonché probabilmente l'unica utilizzabile stante una «*variegata rassegna di usi linguistici in materia*» [2], la definizione contenuta nella Carta etica europea sull'utilizzo dell'Intelligenza Artificiale nei sistemi giudiziari e negli ambiti connessi [3], ove la stessa viene espressa in termini di «*insieme*

[1] Per una efficace ricostruzione della questione, v. L. ALGERI, *Intelligenza artificiale e polizia predittiva*, in *Dir. pen. e proc.*, 6, 2021, ove l'A. afferma che «come disciplina scientifica, l'IA comprende diversi approcci e diverse tecniche, come l'apprendimento automatico (di cui l'apprendimento profondo e l'apprendimento per rinforzo sono esempi specifici), il ragionamento meccanico (che include la pianificazione, la programmazione, la rappresentazione delle conoscenze e il ragionamento, la ricerca e l'ottimizzazione) e la robotica (che comprende il controllo, la percezione, i sensori e gli attuatori e l'integrazione di tutte le altre tecniche nei sistemi ciberfisici)». Per una disamina relativa al concetto di intelligenza artificiale e agli aspetti connessi, v. F. BASILE, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Dir. pen. e uomo*, 10, 2019.

[2] G. UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in *Dir. pen. cont.*, 4, 2020, p. 75 ss. Attesa la difficoltà di rinvenire un significato alla locuzione "intelligenza artificiale", l'A. rinvia, in tema, a un'efficace sintesi dei tentativi in proposito operati da G. ROMANO, *Diritto, robotica e teoria dei giochi: riflessioni su una sinergia*, in G. ALPA (editor), *Diritto e intelligenza artificiale,* Pacini, Pisa, 2020.

[3] *Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi*, adottata nei giorni 3-4 dicembre 2018 dalla Commissione europea per l'efficienza della giustizia (CEPEJ), istituita dal Comitato dei ministri del Consiglio d'Europa nel 2002. Successivamente, una recente Comunicazione del 2018 elaborata dalla Commissione europea, intitolata "*Artificial Intelligence for Europe*" fornisce la seguente definizione di IA: «l'Intelligenza artificiale indica sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi. I sistemi basati sull'IA possono consistere solo in *software* che agiscono nel mondo virtuale (ad esempio, assistenti vocali, *software* per l'analisi delle immagini, motori di ricerca, sistemi di riconoscimento vocale e facciale), oppure incor-

di metodi scientifici, teorie e tecniche finalizzate a riprodurre mediante le macchine le capacità cognitive degli esseri umani».

Sebbene la locuzione *intelligenza artificiale* appaia a tutt'oggi caratterizzata da perduranti difficoltà nel rinvenirne una definizione efficace e unanimemente condivisa, l'aspetto su cui sembra invece esserci concordia concerne le sue principali caratteristiche, desumibili coordinandone i tratti distintivi. In primo luogo, la circostanza secondo cui la stessa, nel suo peculiare funzionamento, si basa sull'utilizzo di ingenti quantità di dati e informazioni. Ancora, il suo caratterizzarsi per un'elevata capacità logico-computazionale in grado di analizzare i dati e le informazioni elaborate. Da ultimo, la peculiare attitudine di assumere decisioni corrette, a seconda del campo di applicazione di riferimento, mediante l'impiego di nuovi algoritmi come quelli del *deep learning* e del *machine learning*, i quali definiscono metodi per estrarre conoscenza dai dati al fine di dotare le macchine dell'abilità di adottare le decisioni adeguate nei vari contesti applicativi, senza escludere una modifica degli algoritmi originari man mano che ricevono più informazioni su quello che stanno elaborando [4].

Atteso tale ultimo riferimento, è opportuno operare un breve richiamo agli algoritmi testé citati, ossia il *machine learning* e il *deep learning*, quest'ultimo quale sottocategoria del primo, descritti come un insieme di algoritmi e metodi di programmazione.

Per *machine learning*, letteralmente *apprendimento automatico* [5], si intende l'abilità di una macchina di apprendere senza essere stata preventivamente ed esplicitamente programmata. Utilizza metodi di reti neurali ispirate al funzionamento del cervello umano, modelli statistici e ricerche operative, al fine di rinvenire le informazioni nascoste nei dati. È un sistema di calcolo costituito da unità interconnesse, come i neuroni, che elaborano le informazioni rispondendo a *input* esterni, trasmettendole tra diverse unità. Si tratta di un sistema in grado di apprendere autonomamente e di imparare dai propri errori basandosi su algo-

porare l'IA in dispositivi *hardware* (ad esempio, in robot avanzati, auto a guida autonoma, droni o applicazioni dell'Internet delle Cose)», COM (2018) 237 final, del 25 aprile 2018.

[4] G. UBERTIS, *op. ult. cit.*; V. anche G. SIMEONE, *Machine Learning e tutela della Privacy alla luce del GDPR*, in G. ALPA (ed.), *Diritto e intelligenza artificiale*, Pacini, Pisa, 2020.

[5] La *Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi* (v. nota 3), definisce così il concetto di *machine learning*: «L'apprendimento automatico consente di costruire, a partire dai dati, un modello matematico che include un gran numero di variabili non conosciute in anticipo. I parametri si configurano gradualmente durante la fase di apprendimento, che utilizza insiemi di dati di addestramento per reperire e classificare i collegamenti. I diversi metodi di apprendimento automatico sono scelti dai progettisti a seconda della natura dei compiti da svolgere (raggruppamento). Tali metodi sono generalmente classificati in tre categorie: apprendimento supervisionato (da un essere umano), apprendimento non supervisionato e apprendimento per rinforzo».

ritmi che analizzano dati; imparando da essi si possono prendere decisioni e condurre previsioni, e il processo di apprendimento avviene attraverso l'analisi di *big data* [6].

Si è inoltre soliti distinguere tre approcci principali di *machine learning*: l'apprendimento supervisionato (*supervisioned learning*), l'apprendimento non supervisionato (*unsupervisioned learning*) e l'apprendimento per rinforzo (*reinforcement learning*) [7].

Il *deep learning,* invece, letteralmente *apprendimento profondo*, è un sottoinsieme del *machine learning*, e come quest'ultimo è un sistema in grado di apprendere autonomamente e imparare dai propri errori, ma ciò avviene sfruttando un sistema complesso di reti neurali che simulano il comportamento cellulare del cervello umano, dalla cui struttura il suddetto approccio trae spunto. Indica quella branca dell'IA che fa riferimento agli algoritmi ispirati alla funzione del cervello, ossia le reti neurali artificiali [8]. Con esso vengono simulati i processi di apprendimento del cervello biologico attraverso le reti neurali, ossia sistemi artificiali, per insegnare alle macchine non solo ad apprendere autonomamente ma a farlo in modo più "profondo", ossia su più livelli, proprio come sa fare la mente umana [9].

Ne deriva che, applicando il *deep learning*, sarà possibile avere una macchina in grado di classificare autonomamente i dati e di strutturarli gerarchicamente, individuando tra gli stessi quelli maggiormente utili o rilevanti ai fini della risoluzione di un dato problema, migliorando le proprie prestazioni con l'apprendimento continuo [10].

Alla luce di quanto sommariamente premesso e virando ora verso il fulcro della presente ricerca, giova evidenziare come le enormi potenzialità apportate dai

[6] Concetti sviluppati sulla scorta di argomentazioni tecniche fornite da personale specificamente competente in servizio presso il Reparto di cui alla successiva nota 12.

[7] Per una disamina dettagliata, v. *L'impatto dell'Intelligenza Artificiale (AI Artificial Intelligence) sul ciclo di intelligence e sugli strumenti a disposizione per i pianificatori militari e le forze dell'ordine*, a cura del Centro Alti Studi per la Difesa – Istituto Alti Studi per la Difesa, 71ª Sessione di studio IASD 2019-2020, pubblicazione a cura del Centro Militare di Studi Strategici. Si veda anche G. SARTOR, F. LAGIOIA, *Le decisioni algoritmiche tra etica e diritto*, in U. RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè Francis Lefebvre, Milano, 2020.

[8] L. ALGERI, *Intelligenza artificiale e polizia predittiva*, cit.

[9] G. SARTOR, F. LAGIOIA, *op. ult. cit*. Con riferimento ai sistemi di *machine learning* e *deep learning*, v. anche *How AI and Machine Learning Are Impacting Digital Investigations*, by O. YOSIFON: *VP of Technology, Cellebrite, White Paper – How Custom Media Categorization are Helping Digital Investigations*, in *www.cellebrite.com*.

[10] Concetti sviluppati sulla scorta di argomentazioni tecniche fornite da personale specificamente competente in servizio presso il Reparto di cui alla successiva nota 12.

sistemi di IA si siano rivelate notevolmente efficaci nel campo delle attività investigative di competenza delle forze di polizia (come anche in quello, ben diverso, dell'*intelligence militare* [11]), settore nel quale l'avvento della stessa è apparso di non poco rilievo, avendo consentito di sviluppare metodologie di indagine utilissime nell'ambito delle attività investigative e della prevenzione dei crimini. Metodologie innovative e dinamiche, basate principalmente sulla raccolta di dati, in grado di rivelarsi particolarmente efficaci in ragione della loro rilevante attitudine a orientare specifici filoni investigativi, attuare strategie di prevenzione e stabilire relazioni e connessioni.

La presente ricerca, condotta con esclusivo riferimento ai sistemi in uso all'Arma dei Carabinieri [12], intende analizzare come e in che misura la rivoluzione tecnologica sulla quale si fondano le nuove tecniche investigative basate sull'IA abbia contribuito ad agevolare le forze dell'ordine nell'espletamento delle tradizionali attività di indagine di propria competenza, nelle quali sono da ricomprendere altresì quelle volte ad attuare strategie di prevenzione dei fenomeni criminali.

[11] Al fine di circoscrivere con precisione cosa si intende per *intelligence* militare, è utile richiamare quanto riportato con riferimento alla nozione in commento in *L'impatto dell'Intelligenza Artificiale sul ciclo di intelligence e sugli strumenti a disposizione per i pianificatori militari e le forze dell'ordine*, cit., ove si legge che «L'Intelligence Militare si pone alla base della capacità di difesa e di pianificazione ed attraverso l'analisi dei dati e delle informazioni raccolte fornisce indicazioni e orientamento per assistere i Comandanti nelle loro decisioni e la sua accuratezza, tempestività e affidabilità, sono essenziali per la riuscita delle operazioni militari». Sempre nel passaggio qui riportato, è inoltre interessante segnalare quanto più avanti precisato con riferimento all'attività di *intelligence* militare, e cioè che: «L'attività di Intelligence Militare si può scomporre da un punto di vista logico in una serie di momenti o fasi costituenti il cosiddetto ciclo di Intelligence, che non si pongono necessariamente in stretta successione ed in cui intervengono attori e si realizzano funzioni diverse». Richiamando solo alcune delle suddette fasi indicate nell'opera citata, si legge che queste «sono costituite rispettivamente da: – pianificazione e direzione in cui gli organi di comando interessati definiscono gli obiettivi informativi ritenuti necessari per le proprie decisioni e che possono attenere al livello strategico, al livello operativo ed al livello tattico (…); – raccolta delle informazioni in cui vengono messe in atto, da parte degli attori/organi preposti, tutte le attività di raccolta dei dati e delle informazioni riferite agli Elementi definiti nella fase precedente; dati ed informazioni vengono raccolti attraverso attività tecniche specifiche a partire da una serie di sorgenti dette fonti». Per ulteriori approfondimenti sul tema, v. p. 58 ss.

[12] La presente ricerca è stata condotta con la collaborazione dell'Arma dei Carabinieri, in particolare del Raggruppamento Operativo Speciale, Reparto indagini telematiche, cui è necessario rivolgere un sentito ringraziamento per il fondamentale apporto fornito. Il presente lavoro costituisce l'esito di una complessa attività di ricerca condotta anche grazie a molteplici colloqui intercorsi con personale specificamente competente in servizio presso il suddetto Reparto. Per ragioni imposte da evidenti esigenze di riservatezza, si precisa che in alcune parti, riferite soprattutto agli strumenti investigativi in uso al Raggruppamento, il lavoro non sarà corredato di nota di riferimento.

Tale ultimo richiamo intende riferirsi al peculiare ambito rientrante nella più generale attività di *law enforcement* finalizzata alla prevenzione e al contrasto dei reati, quello cioè di cd. *polizia predittiva* (o *predictive policing*), il cui scopo è quello, per l'appunto, di *predire,* utilizzando e rielaborando mediante algoritmi una serie di dati e informazioni a disposizione, luogo e tempo in cui potrà essere commesso un reato mediante l'individuazione di zone che presentino maggiore propensione al suo verificarsi (cd. *hotspots*) nonché identificare criminali potenzialmente pericolosi che potrebbero rendersene autori (cd. *crime linking*) [13].

In siffatti contesti, l'impiego dei nuovi strumenti perfezionati grazie all'innovazione tecnologica ha giocato un ruolo strategico, fungendo da fondamentale ausilio alle forze dell'ordine sia con riferimento al contesto strettamente investigativo sia a quello relativo al controllo del territorio e alla sua analisi geografica, con lo scopo di coglierne più agevolmente e con maggiore precisione le dinamiche sociali.

L'intelligenza artificiale si è già candidata a divenire una componente di rilievo nel sistema di difesa e sicurezza pubblica e l'Arma dei Carabinieri, forza militare di polizia a competenza generale e in servizio permanente di pubblica sicurezza con rango di forza armata, il cui tratto distintivo è rinvenibile in una impareggiabile capacità di interpretare il territorio e coglierne le dinamiche in maniera capillare, ha sin da subito colto le enormi potenzialità insite nell'innovazione tecnologica al fine di accrescere ulteriormente la propria efficienza. Istituzione di antica e illustre tradizione, l'Arma si è progressivamente dotata di strumentazioni moderne in linea con l'evoluzione tecnologica, adeguando e integrando in tale ottica i tradizionali mezzi investigativi già in uso [14].

[13] In tema, v. F. BASILE, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, cit.

[14] Per citare solo alcuni degli strumenti investigativi già in uso all'Arma dei Carabinieri, è possibile richiamare, ad esempio, lo SDI (Sistema di indagine), una banca dati sorta con finalità operative contenente informazioni su reati, eventi, autori, vittime e oggetti censiti come documenti, banconote, armi, veicoli, etc. Si tratta di un sistema interforze alimentato da tutte le forze di polizia a utilità comune delle stesse, cui ha possibilità di accedere, pur senza poteri di immissione di dati, anche l'autorità giudiziaria. Il patrimonio informativo dello SDI è costituito dai dati e dalle informazioni derivanti dalle attività di prevenzione e repressione dei reati nonché di tutela dell'ordine pubblico e della sicurezza pubblica. Questa banca dati racchiude le informazioni su fatti, provvedimenti, eventi ed esiti dei controlli sul territorio. In tema, v. P. AGLIECO, *La Banca Dati delle Forze di Polizia*, in *Rass. Arma dei Carabinieri*, 4, 2016, p. 163 ss. Altro strumento utilizzato per il controllo del territorio è il programma SICOTE (Sistema di controllo del territorio), volto ad assicurare un efficace supporto alle attività di prevenzione generale e di controllo territoriale. Ciò ha consentito di estendere notevolmente le capacità analitiche e operative dei reparti volte alle attività informative e di contrasto al terrorismo e alla criminalità organizzata. Ancora, è possibile citare anche l'utilizzo

Attesa l'indubbia utilità di siffatti strumenti, originati dalla rivoluzione tecnologica in commento, è tuttavia necessario considerare che, sebbene molti di essi siano già in uso alle nostre forze dell'ordine, si tratta di sistemi che per quanto innovativi appaiono ancora relativamente "giovani".

Il loro impiego in ambito investigativo è già una realtà ma, stante la loro straordinaria rilevanza in siffatti contesti e trattandosi di strumentazioni efficacemente impattanti sulle attività di investigazione, se ne prevede una intensificazione nei prossimi anni.

8.2. *L'intelligenza artificiale applicata alle attività di polizia. In particolare: il suo impiego nell'ambito delle tradizionali attività di indagine*

Nel procedere con l'analisi delle strumentazioni in uso all'Arma dei Carabinieri, è opportuno sin d'ora precisare come quest'ultima, e in particolare il Raggruppamento Operativo Speciale con il cui apporto è stata condotta la presente ricerca, non possano oggi fare a meno di ricorrere all'utilizzo di strumenti basati sull'intelligenza artificiale e delle metodologie da essa derivanti.

Tali strumenti si differenziano nettamente da quelli convenzionalmente adoperati nell'ambito delle attività investigative, caratterizzate dal fatto di seguire un approccio tradizionale.

Nel contesto attuale, la presenza sempre maggiore di dati a disposizione, come quelli prodotti da uno *smartphone* o da un computer che, costantemente connessi alla rete, raccolgono e inviano dati idonei a rivelare informazioni talvolta preziose per gli inquirenti, è una delle ragioni che consente di utilizzare le tecnologie in argomento.

di un peculiare apparato denominato ODINO (*Operational device for information, networking and observation*), in grado di incrementare qualità e quantità dei controlli su strada. Si tratta di tablet impiegato in molteplici tipologie di scenari operativi munito di navigatore satellitare integrato e radiolocalizzato presso la centrale operativa, su cui sono installate app per l'accesso al sistema interforze SDI, sopra citato, nonché alle banche dati a valenza info-investigativa, al fine di trasmettere alla centrale messaggi, immagini o video acquisiti. Con riferimento al settore del *cybercrime*, l'esigenza di sviluppare nuove capacità di contrasto al crimine informatico in tutte le sue forme ed evoluzioni, ha reso necessaria l'assunzione di idonee contromisure da parte del ROS e dei nuclei investigativi, individuando strumenti tesi a potenziare le competenze nel settore dell'investigazione digitale. In tale ambito, sono stati sviluppati servizi di *deciphering*, con la realizzazione di sistemi prototipali volti alla decodifica di comunicazioni IP, attualmente in uso su diverse piattaforme applicative. In tema, o anche con rifermento ad altre strumentazioni in uso, v. *Carabinieri, tutte le nostre tecnologie per la sicurezza del territorio*, 2018, consultabile in *www.agendadigitale.eu*.

Le informazioni estrapolate dai dati raccolti possono infatti essere efficacemente adoperate dagli operatori di polizia, i quali sono in grado di valorizzarle al fine di creare strumenti di ausilio nello svolgimento delle attività investigative.

È necessario sin d'ora evidenziare come la conoscenza di nuova generazione, figlia dei moderni sistemi di intelligenza artificiale, consenta allo stato attuale agli operatori appartenenti al comparto di *law enforcement* che svolgono indagini, di poter proseguire nelle stesse raggiungendo gli obiettivi investigativi di interesse celermente e con notevole efficacia.

Lo svolgimento di un'attività investigativa, a prescindere dal grado di complessità, pone all'attenzione degli operatori un'ingente quantità di dati e di informazioni, la cui conoscenza è fisiologica nell'ambito di una tradizionale investigazione.

È sufficiente in tal senso immaginare i dati di cui si è in grado di disporre analizzando tabulati telefonici, intercettazioni telematiche, telefoniche e ambientali, file di *log* di dispositivi, account di sistemi informatici o di *social network*, immagini audio o video raccolte da un cellulare, il contenuto di una *chat*, la lista passeggeri di un treno riguardante una determinata tratta attenzionata, e tutto con riferimento a periodi temporali talvolta lunghissimi.

Notevole rilevanza assumono in tale contesto proprio le intercettazioni sia di comunicazioni telefoniche sia ambientali, come anche l'utilizzo dei cd. captatori informatici, ovvero di applicazioni *software* che vengono installate da remoto sui dispositivi mobili personali del soggetto di interesse investigativo a sua insaputa, con lo scopo di ricavarne dati e informazioni. Tali strumentazioni costituiscono metodi investigativi particolarmente efficaci e si caratterizzano per il fatto di generare i maggiori volumi di dati e di informazioni.

È interessante evidenziare come i dati così ottenuti si presentino per lo più come non strutturati, e che la parte fondamentale del processo di estrazione di conoscenza dagli stessi si sviluppi analizzando i testi ottenuti dalle trascrizioni del materiale ricavato mediante le intercettazioni. A tal fine, costituisce un valido ausilio l'impiego di tecniche criptografiche.

Da quanto esposto deriva che un'eccessiva quantità di notizie gestite in maniera inadeguata o confusionaria porterebbe con sé il rischio di ingarbugliare pericolosamente i percorsi investigativi inducendo a risultati fuorvianti, comportando il verificarsi proprio di ciò che è invece opportuno evitare nel corso dello svolgimento di un'indagine.

Tale situazione aumenterebbe senz'altro le difficoltà già di per sé ontologicamente insite in un'attività investigativa senza condurre ad alcun risultato utile per gli investigatori, implicando, per converso, il manifestarsi del fenomeno noto come *crazy wall*, connesso con l'immaginario di una *detective story* americana, in cui l'investigatore si ritrova dinanzi alla parete del proprio ufficio costellata di documenti, mappe e fotografie, legate da fili rossi o da linee scomposte

tracciate con pennarelli. Il carico mentale che ciascun investigatore è chiamato a sostenere rischia di divenire ingestibile, poiché più ci si addentra nel lavoro di indagine e più le informazioni, gli autori coinvolti, i legami e le relazioni si articolano in modo vario e diversificato.

Tutto ciò genera sovente un eccessivo ed elevato *overhead cognitivo* in danno dell'inquirente, tale da rendere ostica la focalizzazione su aspetti rilevanti che potrebbero sfuggire all'analisi dei fatti.

Spesso si è a un passo dalla risoluzione di un'indagine, dalla svolta, eppure manca l'ultimo tassello del *puzzle* da incastrare al posto giusto, quella intuizione investigativa che, rivelatasi risolutiva, consente di chiudere il cerchio. O magari potrebbe accadere l'esatto contrario, e cioè che, giunti al momento decisivo, ci si accorge di aver intrapreso un percorso errato, o del fatto che l'intera piattaforma indiziaria e probatoria appare improvvisamente propendere per una soluzione antitetica a quella che fino a poco prima sembrava essere la chiave di volta per la risoluzione del problema.

In entrambi i casi, gli strumenti basati sulla IA si rivelano essere di estremo aiuto nella conduzione o nel mutamento di prospettiva di un'indagine, sia nella sua conclusione sia nel momento in cui ci si accorge di dover invertire la direzione intrapresa e orientarsi in altro senso.

Occorre dunque dare atto di come l'evoluzione tecnologica applicata al contesto investigativo si sia rivelata sin da subito di estremo ausilio in occasione della repressione di molteplici fenomeni criminali.

È evidente come le organizzazioni criminali, evolvendosi, siano oggi sempre più in grado di investire risorse e di estendere le proprie radici verso ogni latitudine, di tessere relazioni in ambienti rilevanti e differenti, essendo alla perenne ricerca, purtroppo in grado di rivelarsi spesso fruttuosa, di terreni economicamente fertili. I fenomeni criminali hanno sempre manifestato particolare attitudine nell'adeguarsi al contesto sociale e al momento storico di riferimento grazie a una spiccata capacità di coglierne minuziosamente evoluzioni o mutamenti (basti pensare all'attuale fase pandemica, caratterizzata dalla costante attività di infiltrazione da parte di tali organizzazioni in settori particolarmente critici) ma anche, e soprattutto, all'avanzare e al costante sviluppo delle moderne tecnologie.

Il comparto del *law enforcement*, la cui missione è quella di ricercare, inseguire, individuare, contrastare e debellare fenomeni criminali e illeciti penali in generale, di tutto ciò è assolutamente consapevole. In tale prospettiva, gli organi inquirenti sono ben consci del fatto che il passaggio dalla tradizionale investigazione condotta ricorrendo a strumenti convenzionali a quella "digitale" agevoli nettamente il proprio lavoro, velocizzando e semplificando i processi decisionali.

Risulta dunque evidente che, se da una parte sono le organizzazioni criminali ad adeguarsi alle tecnologie che si evolvono, dall'altra sono gli organi inquirenti a doversi "adeguare" alle organizzazioni criminali e alla realtà che le caratteriz-

za. E ciò sta oggi accadendo, atteso che, in ausilio al comparto di *law enforcement* e alla risoluzione delle indagini, accorre la *computer science* e le rispettive sottodiscipline, tra le quali, in particolare, l'intelligenza artificiale.

Poste tali doverose premesse e prima di scendere nell'analisi dei molteplici possibili ambiti applicativi dell'intelligenza artificiale in un contesto investigativo, è altresì necessario soffermarsi sul diverso e peculiare approccio che si rivela necessario adottare nella risoluzione di specifiche problematiche, o *task*, nel campo dell'intelligenza artificiale.

In tale settore non si dispone di un algoritmo prefissato che, sulla scorta degli *input* disponibili, ricavi gli output desiderati. Spesso, infatti, la soluzione va elaborata nel corso dell'indagine *in fieri*. Si procede a una valutazione complessiva delle soluzioni percorribili, prediligendo quella che si ritiene essere idonea alla definizione del problema.

Con riferimento all'IA, si ricorre spesso ai cd. *agenti intelligenti*, resi operanti nell'ambiente di interesse e muniti di una *base di conoscenza*, di diversi meccanismi di elaborazione, di ragionamento e di immagazzinamento dati, il cui scopo è quello di interagire con l'ambiente e con gli attori lì operanti portando a termine i *task* necessari al raggiungimento dell'obiettivo primario.

L'*agente* è dotato di sensori mediante i quali è in grado di percepire gli accadimenti del contesto circostante e come esso si caratterizza; di attuatori che consentono di porre in essere azioni di svariate tipologie (motorie e non); di una componente "intelligente" che permette di procedere ad un'elaborazione dei dati raccolti e di intraprendere azioni sulla scorta di *decisioni* adottate. L'*agente* è altresì in grado di modificare la lettura dell'ambiente prima ricavata e le conseguenti azioni da intraprendere, dunque di "aggiornare" le proprie conoscenze adeguandosi agli elementi successivamente emersi dall'esame del contesto considerato. Sostanzialmente, al pari di un essere intelligente, lo stesso può anche "ritornare sui propri passi" (ossia, andare in *backtracking*), percorrendo quindi un itinerario diverso da quello prima intrapreso, per sceglierne un altro considerato come migliore e più utile per il raggiungimento dell'obiettivo primario [15].

È inoltre possibile individuare tre diversi approcci per la risoluzione di un problema da valutare.

Il primo è il cd. *approccio imperativo,* ossia quello classico, il cui schema è riassumibile nella formula *programma (o algoritmo) = strutture dati + istruzioni.*

Due distinte modalità di approccio vengono invece impiegate nel campo dell'IA, e cioè: a) il cd. *approccio dichiarativo*, il cui schema è riassumibile nella formula *programma (o algoritmo) = logica (base di conoscenza) + controllo*

[15] Concetti sviluppati sulla scorta di argomentazioni tecniche fornite da personale specificamente competente in servizio presso il Reparto di cui alla nota 12.

(motore inferenziale, le regole); b) il cd. *approccio per apprendimento*, il cui schema è invece riassumibile nella formula *programma (o algoritmo) = Esempi (esperienza, base di conoscenza) + machine learning (modello di apprendimento)*. In quest'ultimo approccio è altresì possibile operare un'ulteriore distinzione tra *apprendimento supervisionato, apprendimento non supervisionato* e *apprendimento per rinforzo* [16].

Alla luce di quanto sin qui delineato, si evidenziano ora nel dettaglio i molteplici possibili ambiti applicativi dell'intelligenza artificiale in un contesto investigativo.

Occorre in primo luogo porre in risalto la capacità di talune strumentazioni, nell'ambito della *computer vision*, di procedere alla categorizzazione delle immagini: in tal senso, è possibile determinare con precisione se si tratti dell'immagine di una persona, di un animale, di un oggetto oppure di una macchina, di un edificio, di una droga, di un esplosivo, di un'arma, etc., precisando quali. Detti strumenti consentono inoltre di analizzare le immagini, di cercare, individuare e ricavare elementi di interesse in esse contenuti, come la targa di una vettura; consentono inoltre di procedere alla pulizia e al filtraggio delle stesse, come pure di provvedere alla loro comparazione, al fine di rinvenire similitudini o analogie nel contesto di interesse.

Ancora, sempre con riguardo all'ambito delle raffigurazioni visive, tali strumentazioni consentono di comparare due immagini della medesima tipologia, fornendo come risultato uno *score* di similitudine, per verificare, ad esempio, se due immagini di persona rappresentino o meno il medesimo soggetto. È inoltre possibile individuare, procedendo a un'accurata analisi dell'immagine di riferimento, l'esatto momento temporale corrispondente al verificarsi di un determinato evento, come anche determinare quale sia il luogo di interesse, oppure ricavarne la descrizione di un'attività in corso di svolgimento o di una precisa circostanza sulla scorta del contenuto della raffigurazione (ad esempio, determinare che l'evento in questione sia avvenuto di mattina piuttosto che di notte, presso una scuola, un parco, una nave, oppure durante una festa, una rapina o una discussione).

Dai possibili contesti applicativi ora individuati, risulta di particolare interesse il cd. *task di age progression*, il quale consente, acquisita l'immagine del volto di una determinata persona, di procedere alla riproduzione/ricostruzione delle sembianze della stessa a distanza di tempo, di anni se si tratta di persona adulta o addirittura di mesi o settimane qualora si tratti di un bambino.

Tale metodologia trova frequente impiego nell'ambito delle attività investigative. Ne fungono da esempio molteplici casi eclatanti di cronaca giudiziaria

[16] *Ibidem*.

aventi ad oggetto la scomparsa di minori, ove, nell'intento di facilitare le ricerche degli stessi anche a distanza di un consistente lasso temporale, si è provveduto a ricostruirne il possibile aspetto fisico e le sembianze del volto nel modo più dettagliato possibile (come accaduto nei noti casi giudiziari relativi alla scomparsa delle piccole Denise Pipitone in Sicilia e Angela Celentano in Campania).

Sempre con riferimento alla metodologia ora richiamata, è rilevante evidenziare come la stessa sia parimenti adoperata in altri contesti, e precisamente quando, acquisita la sequenza audio di una persona, può rivelarsi utile riprodurne la voce anche a distanza di molti anni, riuscendo spesso efficacemente a ricostruire la voce di un bambino immaginandone il possibile sviluppo nel tempo.

Tale precisazione, riferita al già citato *task di age progression*, adoperato questa volta con riferimento al campo degli audio, consente ora di pervenire alla ricognizione degli altri strumenti adoperati nel suddetto settore.

In tale ambito, gli strumenti a disposizione consentono, grazie all'analisi di un determinato audio di interesse investigativo, di procedere efficacemente alla identificazione degli attori presenti sulla scena come pure di comprendere se, nel contesto preso in esame, si sia verificato un preciso avvenimento ovvero siano state poste in essere determinate azioni e quali siano i soggetti che delle stesse si sono resi autori. È altresì possibile, per effetto di queste strumentazioni, risalire alla dinamica e al susseguirsi degli eventi interessati, come lo svolgimento e il conseguente sviluppo di una discussione verbale tra persone poi degenerata in una rissa, o anche ricostruire la genesi e l'evoluzione di uno scontro violento verificatosi in occasione di una partita di calcio, etc.

L'analisi degli audio in possesso consente poi agli operatori di polizia di provvedere all'estrazione del parlato e alla conseguente rappresentazione di una conversazione in formato testo, anche considerando le diversità linguistiche dei soggetti interessati.

Con riferimento poi al diverso settore dei video, è possibile richiamare strumenti e metodologie che consentono di svolgere tutti i *task* sino ad ora descritti, utilizzando, nel caso di specie, i *frame* di cui un video è composto. Analogamente a quanto già riportato con riguardo al settore degli audio, anche in tale contesto è possibile, attraverso un'analisi dettagliata delle immagini video, procedere alla identificazione dei soggetti presenti, alla ricostruzione degli eventi così come svoltisi in quel determinato contesto, ovvero verificare se nello stesso sono state poste in essere determinate azioni e da chi. È inoltre possibile procedere, sempre attraverso l'analisi del video attenzionato, alla estrazione di audio dallo stesso, al fine di convertirlo nel corrispondente formato testuale.

Altro aspetto di interesse concerne il campo dei dati presenti in collezioni massive di documenti testuali, come una mail, una *chat*, un post o un documento HTML (i cd. dati non strutturati), i quali possono talvolta rivelarsi particolarmente rilevanti o utili ai fini di un'indagine in corso.

In tale contesto, le strumentazioni attualmente a disposizione degli inquirenti consentono di operare in molteplici direzioni. In primo luogo, è possibile procedere a una indicizzazione dei documenti e alla loro categorizzazione nonché estrarre uno o più documenti analizzando le richieste effettuate dagli utenti. Un documento è rilevante o attinente qualora soddisfi il bisogno di informazione che l'utente ha manifestato con la sua *query di ricerca*.

Ancora, le strumentazioni attualmente in uso consentono di estrarre semantica da un corpus di documenti, ad esempio attori coinvolti o eventi rappresentati, o anche azioni eseguite e rispettivi autori, e a tal fine, vengono generalmente impiegate tecniche di *Natural language processing* o anche NLP (elaborazione del linguaggio naturale).

È altresì possibile prevedere il potenziale sviluppo di una determinata questione partendo da una data situazione di riferimento quale può essere un'imminente votazione politica o una campagna elettorale, le quali potrebbero comportare rischi per le persone, per i luoghi o addirittura per l'ambiente.

Spostandoci ora nel campo dei dati (*semi*)strutturati, come quelli presenti in database, in file XML, quelli ricavati da siti *web* e dai metadati ivi presenti o anche ricavati da file di *log* dei dispositivi e delle applicazioni che vengono eseguite su di essi, gli strumenti in commento consentono di potersi orientare in varie direzioni.

È cioè possibile: – estrarre conoscenze utili mediante procedure quali regole di associazione, alberi di decisione, funzioni di regressione e predizione e in generale algoritmi di *data meaning*, tutte procedure frequentemente utilizzate nella profilazione degli utenti; – ricavare dai dati a disposizione entità o relazioni e interconnetterle tra loro generando legami gerarchici o persino ereditari; – estrarre conoscenza dai *big data* grazie all'utilizzo di strumentazioni di nuova generazione messe in campo dall'*intelligenza computazionale*, come ad esempio gli *algoritmi genetici* o le *reti neurali profonde* [17].

Quanto evidenziato si può riassumere, in estrema sintesi, affermando che vengono svolte procedure di *big data analytics* [18], e cioè estraendo conoscenza dalla

[17] *Ibidem*.

[18] La Commissione europea [COM (2014) 442 Final] ha definito i *big data* come «una grande quantità di tipi diversi di dati prodotti con un'alta velocità da un grande numero di fonti di diverso tipo. La gestione di tali aggregati di dati richiede oggi nuovi strumenti e metodi, come processori potenti, *software* e algoritmi». I cd. *big data* hanno le seguenti principali caratteristiche, dette anche "5V". Il *volume*, che indica l'enorme quantità di dati; la *velocità*, che indica l'accelerazione nell'elaborazione dei dati; la *varietà*, che rimanda all'eterogeneità delle fonti da cui provengono; la *veridicità*, che sottolinea l'importanza di stabilire la possibile autenticità o inautenticità dei dati; la *variabilità*, che è propria dei dati che emergono in formati diversi e che provengono da contesti diversi. La mutevolezza del loro significa-

enorme quantità di dati che in ogni istante viene generata dai moltissimi dispositivi interconnessi e dalle informazioni immagazzinate nelle sorgenti dati, di natura pubblica e privata.

In linea generale, l'Arma dei Carabinieri ha già da tempo avviato un processo di riorganizzazione e di *informatizzazione*. Quest'ultimo, attesa la sua complessità, è tuttora in fase di completamento e di assestamento nonché destinato ad evolversi ulteriormente nei prossimi anni, proprio in ragione dell'avanzare delle tecnologie [19].

Posta la natura di organizzazione dell'Arma dei Carabinieri – nel caso di specie, militare con funzioni di polizia – si è riscontrato come anche per la stessa non possa prescindersi da una risorsa di rilievo caratteristica di tutte le organizzazioni: l'*informazione*.

Ciò stante, risulta essenziale l'esistenza di un efficiente *sistema informativo* che attenga alla gestione delle informazioni, il quale consente di raccoglierle, archiviarle, gestirle, lavorarle e scambiarle nonché comunicarle all'interno e all'esterno dell'organizzazione stessa.

Diversamente, il *sistema informatico* è quella parte del sistema informativo che riesce a trattare l'informazione una volta contestualizzato il dato e che consente di automatizzare e velocizzare la produzione dei dati e lo scambio di flussi informativi, dunque di coadiuvare il processo decisionale [20].

Il vantaggio di avere un sistema informatico deriva dalla sua efficienza, sicurezza, velocità e minimizzazione sia degli errori sia della perdita dei dati.

8.3. *I sistemi di intelligenza artificiale in uso al Raggruppamento Operativo Speciale dei Carabinieri*

Il Raggruppamento Operativo Speciale (ROS) [21] dispone di strumenti che consentono di pervenire al raggiungimento degli obiettivi necessari con modalità efficaci e con limitatissimi margini di errore.

to è un aspetto da tenere in considerazione nel momento in cui i dati vengono interpretati, v. L. ALGERI, *Intelligenza artificiale e polizia predittiva*, cit. Si veda anche G. DELLA MORTE, *Big data e protezione internazionale dei diritti umani. Regole e conflitti*, Editoriale scientifica, Napoli, 2018; L. PALAZZANI, *Dalla bio-etica alla tecnoetica: nuove sfide del diritto*, Torino, 2017 e U. RUFFOLO, *Intelligenza Artificiale, machine learning e responsabilità da algoritmo*, in *Giur. it*., 2019.

[19] Concetti sviluppati sulla scorta di argomentazioni tecniche fornite da personale specificamente competente in servizio presso il Reparto di cui alla nota 12.

[20] *Ibidem*.

[21] Il Raggruppamento Operativo Speciale (ROS) è stato istituito il 3 dicembre 1990, con

il medesimo provvedimento di legge con cui sono stati costituiti i Servizi centrali ed interprovinciali di Polizia giudiziaria, della Polizia di Stato (SCO) e della Guardia di Finanza (SCICO). All'atto della sua costituzione, il ROS assorbì la preesistente struttura anticrimine dell'Arma, nata a Torino nel maggio del 1974 con un "Nucleo speciale di polizia giudiziaria", – il Nucleo Scintilla – costituito da appena 40 unità appositamente prescelte dal Generale Carlo Alberto dalla Chiesa per l'espletamento di particolari e complesse indagini a livello nazionale. In breve tempo la speciale struttura si impose per l'innovativo metodo investigativo, incentrato sull'approccio sistemico alle matrici criminali e alle rispettive organizzazioni più che sul raggiungimento di successi parziali, seppur importanti: il perseguimento dei reati fine. Strumenti investigativi come le osservazioni, i pedinamenti e le intercettazioni ora consolidati nel cosiddetto metodo anticrimine, vennero sviluppati e via via affinati per identificare i membri delle formazioni eversive e i loro contatti, risalendo progressivamente ai vertici. La struttura del Nucleo Speciale venne nel tempo ampliata, con la costituzione delle sezioni anticrimine con competenza interprovinciale e compiti di contrasto alla criminalità organizzata e ai fenomeni eversivi, strettamente coordinate attraverso la condivisione delle informazioni e delle procedure operative. Il metodo anticrimine, che contribuì agli inizi degli anni 80 alla disarticolazione dei più importanti gruppi terroristici attivi in Italia, quali le Brigate Rosse, Prima Linea, Nuclei Armati Rivoluzionari, venne, poi, adottato per il contrasto a qualsiasi forma di criminalità organizzata. L'obiettivo principale rimase quello di conoscere prima in maniera approfondita il fenomeno, il gruppo criminale, per procedere quindi alla sua disarticolazione. Con riferimento all'aspetto organizzativo, il ROS, il cui comando è conferito a un Generale di divisione/brigata, è articolato su una struttura centrale e una periferica. Alle dirette dipendenze del comandante operano, con competenza nazionale, il: – *Reparto antiterrorismo*, che definisce per l'Arma il quadro della minaccia eversiva e terroristica orientando e coordinando le attività informative e investigative svolte dai reparti e dalle sezioni anticrimine congiuntamente all'organizzazione territoriale, assumendo, se necessario, la direzione delle indagini nei casi di preminente rilevanza anche internazionale. Assicura, inoltre, lo scambio info-operativo con i collaterali organi di polizia nazionali ed esteri operanti nello specifico settore; – *Reparto indagini tecniche*, che garantisce la ricerca e la sperimentazione delle attrezzature per le investigazioni, realizzando periodici scambi informativi con le polizie straniere specializzate nel settore, fornendo supporto tecnico-operativo alle articolazioni periferiche del raggruppamento e dell'organizzazione territoriale; – *Reparto indagini telematiche*, istituito nel febbraio 2015 che rappresenta il "polo centrale" di riferimento per l'Arma dei Carabinieri nel contrasto alla criminalità informatica, nello studio e sperimentazione delle tecnologie per l'esplorazione del *web* e l'intercettazione dei flussi telematici; – *Reparto crimini violenti*, istituito nel 2012, che assicura il potenziamento delle capacità investigative e di intervento dell'Arma dei Carabinieri in occasione di crimini particolarmente efferati che suscitano clamore nella pubblica opinione e nei casi in cui la scomparsa di persone può essere correlata ad un crimine. Alle dirette dipendenze del vice comandante, oltre che le articolazioni periferiche sono posti i 3 reparti del servizio centrale di polizia giudiziaria: – *I Reparto investigativo*, che concorre alle indagini in materia di criminalità organizzata di tipo mafioso e cattura dei latitanti di massima pericolosità, nonché alle attività di ricerca e sequestro dei beni di provenienza illecita nel quadro della speciale normativa antimafia; – *II Reparto investigativo*, che concorre alle indagini in materia di traffico di armi e sostanze stupefacenti, sequestri di persona, riciclaggio, criminalità multietnica e tratta di esseri umani. Provvede, inoltre, all'analisi dei fenomeni di narcotraffico, attuando il collegamento con la dire-

Tra questi, alcuni risultano di mero supporto per le attività svolte dagli operatori in forza presso il Raggruppamento, mentre altri appaiono indispensabili per il prosieguo delle azioni di competenza, la cui assenza comporterebbe vistosi rallentamenti nello svolgimento delle indagini.

Occorre comunque precisare che non tutti gli strumenti attualmente in uso si basano sull'intelligenza artificiale, adottando, gran parte degli stessi, il tradizionale approccio deterministico (nel senso che effettuano una serie di passi prefissati al fine di ricavarne un risultato).

Altri, invece, impiegano l'intelligenza artificiale per effettuare alcuni *task* determinati.

Rientrano in quest'ultima categoria tre tipologie di strumenti attualmente adoperati dal Raggruppamento, e cioè: a) lo strumento di analisi delle immagini; b) lo strumento di analisi del testo ed elaborazione del linguaggio naturale; c) lo strumento per analisi del parlato e *speech recognition* [22].

8.3.1. *Lo strumento di analisi delle immagini*

Nello strumento di analisi delle immagini, il *task* è quello della classificazione. Il suo funzionamento può riassumersi nei seguenti termini: data un'immagine di *input*, il sistema verifica se la stessa appartiene a una delle categorie conosciute (ad esempio, per la persona, se uomo o donna o se bambino o adulto; se si tratta di arma, di denaro, di animale, di droga, di sangue, etc.).

Il sistema viene predisposto per un bacino molto ampio di immagini, dell'ordine delle migliaia per ogni categoria, generando un modello di apprendimento che sarà successivamente adoperato per classificare l'immagine di *input*. Detto sistema, in base ad un cd. *training set*, cioè un complesso di immagini già etichettate o delle quali si conosce già la categoria, crea un modello di apprendimento che verrà in seguito utilizzato dallo stesso quando gli si presenteranno immagini di *input*.

zione centrale dei servizi antidroga del Ministero dell'Interno per tutte le attività investigative in materia di stupefacenti condotte dall'Arma dei Carabinieri; – *III Reparto analisi*, che svolge attività di analisi e ricerca operativa sulle manifestazioni della criminalità organizzata, assicurando il supporto informativo alle attività investigative del ROS, mantenendo i rapporti con organismi nazionali ed esteri che si occupano di studio ed analisi dei fenomeni criminali. Partecipa a progetti di analisi interforze sui fenomeni criminali individuati dalle "conferenze dei servizi centrali di polizia giudiziaria". La struttura anticrimine periferica è articolata in 8 reparti anticrimine (Torino, Milano, Roma, Bari, Napoli, Catanzaro, Reggio Calabria e Palermo) e 18 sezioni anticrimine, collocate in sede di procure distrettuali antimafia e antiterrorismo nonché 3 nuclei a Livorno, Nuoro e Foggia. Le informazioni qui riportate sono tratte dal sito ufficiale dall'Arma dei Carabinieri, *www.carabinieri.it*.

[22] Concetti sviluppati sulla scorta di argomentazioni tecniche fornite da personale specificamente competente in servizio presso il Reparto di cui alla nota 12.

8.3.2. *Lo strumento di analisi del testo ed elaborazione del linguaggio naturale*

Questo strumento è contraddistinto da una forte componente di intelligenza artificiale, risultando al suo interno elementi che assolvono a differenti *task* effettuabili su documenti e su testi ivi compresi.

È possibile gestire file testuali in formati differenti (un PDF, TXT, HTML, CSV, etc.) e in varie lingue. Nello svolgere i diversi *task*, il sistema in argomento impiega moduli che vengono richiamati per svolgere l'analisi testuale (lessicale e semantica) ricevendo come *input* dati non strutturati, (principalmente mero testo) e restituendo come output dati strutturati, quindi conoscenza, che costituiscono l'esito dell'analisi per mezzo delle tecnologie di IA.

I moduli di cui è composto il sistema e che adoperano l'IA, sono di seguito precisati.

Il primo è costituito dall'*estrattore delle parole chiave (le keyword)*, il quale consente di ricavare le parole chiave presenti nei documenti. L'estrazione automatica di dette parole chiave assegnerà automaticamente i termini di indicizzazione al fine di facilitare il recupero. L'output di questo modulo è costituito da una lista dei termini presenti nei documenti con associato ad ogni termine il relativo numero di occorrenze (un *text rank*). A ogni termine viene assegnato un certo "peso" per comprendere quali siano stati utilizzati maggiormente e quali siano invece stati adoperati con minore frequenza. Le modalità di visualizzazione dell'output di questo modulo sono molteplici.

Oltre a una mera lista, altra modalità è rappresentata da un grafico a barre; un'altra ancora è costituita dalla visualizzazione dei termini attraverso una *word cloud*, ove i termini più grandi e visibili presentano un elevato numero di occorrenze nel testo, mentre quelli raffigurati come più piccoli e sottili, ne hanno di meno.

Proseguendo, il secondo modulo è costituito dall'*estrattore delle entità (named entity recognition).*

Tale modulo consente di ricavare le entità dal documento e attribuisce un'etichetta sulla scorta della classe di appartenenza. Le entità estratte presentano un tag associato che ne costituisce la tipologia. Ad esempio, qualora nel testo compaia "Rossi Mario", ad esso verrà associata l'entità *persona*, mentre qualora compaia "4/10/2020", ad esso verrà associata l'entità *data*. Alcune delle entità estratte possono essere le seguenti: persona, prodotto, arma, data, quantità, moneta, evento, città, etc.

Task di summarization

Questo modulo ha la finalità di ricavare un riassunto quanto più ricco e completo possibile dal testo di un documento in modo da non alterare la semantica

del testo originale ma riducendo lo sforzo che l'operatore deve compiere per comprenderne il contenuto.

Questo *task* si divide in due categorie: – *estrattivo*, in cui il testo viene riassunto eliminando frasi o parti di esse, lasciando quelle più rilevanti o importanti con riferimento a ciò che il testo cerca di esprimere; – *astrattivo*, in cui il testo viene riassunto sostituendo i termini che contiene (verbi, soggetti, complementi oggetto, etc.) con altri simili dal punto di vista semantico, lasciando inalterato il contenuto informativo generale del testo stesso. Diversamente dal precedente, il riassunto *astrattivo* non si limita a copiare frasi importanti dal testo di origine, ma tenta di fornire anche nuove frasi rilevanti. In sostanza, si adoperano frasi diverse da quelle presenti nel testo, per esprimere i concetti.

Topic extractor

Questo modulo ricava i *topic* principali da un documento. Le parole dal significato semantico simile vengono riunite in rettangoli colorati, che rappresentano i *topic*. Viene svolta un'attività di *clustering* sul testo. Spetterà poi all'operatore comprendere a cosa il *topic* (rettangolo colorato) faccia riferimento.

Conoscenza in forma di grafo

Questo modulo produce un grafo orientato, cioè una mappa della conoscenza, dove i *nodi*, che rappresentano le entità ricavate dal testo, sono collegati da archi che rappresentano relazioni e azioni tra le entità. Ciò consente di rappresentare le connessioni e le relazioni (tassonomie e gerarchie) che sono comprese nel testo e le entità interessate (con generalizzazioni e specializzazioni).

Analisi del sentiment

Questo modulo consente di conoscere il livello di considerazione, interesse e soddisfazione, verso determinate questioni, eventi accaduti, persone, prodotti, animali. Esso conferisce un'etichetta relativa a un livello di considerazione a una sequenza di testo, rappresentando in tal modo il *sentiment* associato.

8.3.3. *Lo strumento per analisi del parlato e* speech recognition

Tale sistema, dato un determinato file audio in diversi formati (MP3, PCM, WMA, WAV, etc.), permette di pulire, filtrare e ricavare il parlato da un estratto audio. Il sistema genera dai file audio dati non strutturati (mero testo) e dati (semi)strutturati. A questo punto, esso può impiegare dei sottomoduli per procedere con successive elaborazioni sulla differenziazione della tipologia di dato.

Questo risulta essere allo stato attuale il complesso delle strumentazioni, basate sulla tecnologia in commento, a disposizione del ROS per perseguire effi-

cacemente, con pochissimi margini di errore e considerevoli risparmi di tempo, gli obiettivi investigativi di interesse.

8.4. *Riflessioni conclusive*

Il contesto sin qui emerso consente di rilevare come, al giorno d'oggi, la nostra vita sia costantemente e continuamente dominata dall'intelligenza artificiale, qualunque sia l'attività che si renda necessario intraprendere nel corso della giornata.

L'incessante e rapido evolvere delle tecnologie, se da un lato è in grado di trasmettere una maggiore sicurezza derivante dal fatto che le stesse sono in grado di offrire strumentazioni aggiornate e prontamente adoperabili, dall'altro prospetta uno scenario per certi versi non del tutto tranquillizzante, stante l'invadenza con la quale siffatte tecnologie hanno prepotentemente fatto irruzione nella nostra quotidianità.

Con riferimento all'aspetto che qui maggiormente interessa, giova evidenziare che l'esito della ricerca consente di constatare come l'impiego delle tecnologie basate sulla IA si sia rivelato particolarmente incisivo nel campo delle attività investigative, offrendo agli organi inquirenti strumentazioni e metodologie efficacemente adoperabili in siffatti contesti e a svariati fini, certamente in grado di agevolare il loro lavoro [23].

Si tratta, come visto, di sistemi di nuova generazione [24], non molti e recentemente approntati, tuttavia in grado di raggiungere gli obiettivi di interesse investigativo con pochissimi margini di errore e con grande precisione, siano essi strumenti di mero ausilio agli uomini che li adoperano piuttosto che indispensabili ai fini del prosieguo delle attività di indagine.

L'attività investigativa si è dunque anch'essa ritrovata, come pure altri campi del diritto penale [25], a dover fare i conti con l'impetuoso irrompere dell'innova-

[23] V. *supra*, § 1.

[24] V. *supra*, § 2.

[25] Oltre a quello avente ad oggetto le attività di *law enforcement* e in particolare quelle di polizia predittiva, il possibile impiego di sistemi basati sull'intelligenza artificiale viene altresì in rilievo in ulteriori e distinti ambiti del diritto penale. In primo luogo in quello giudiziario, e segnatamente con riferimento alla possibilità di adoperare algoritmi decisionali, i cd. *automated decision systems*, al fine di risolvere le controversie. Tali algoritmi decisionali sono stati prevalentemente adoperati per questioni di natura civilistica, ma nulla esclude che possano essere presto impiegati anche nel settore penale, rispetto al quale si discute in merito alla possibilità (e alla ragionevolezza) di realizzare una sorta di sostituzione, o comunque di affiancamento, del giudice-uomo col giudice-macchina. Altro ambito rispetto al quale si di-

zione tecnologica, indubbiamente rivelatasi, anche in tale ambito, notevolmente impattante. E la transizione dall'investigazione tradizionale a quella "digitale" non è stata automatica, poiché, come evidenziato, siffatto passaggio ha reso necessario adottare un differente approccio da parte degli organi inquirenti nell'impiego della stessa [26].

È dunque possibile constatare come il ricorso a questa metodologia di indagine risulti oggi sempre più diffuso nell'attuale panorama investigativo e che l'utilizzo di tecniche di IA sia divenuto sempre più pervasivo, sino a costituire, in talune ipotesi «*l'unica prospettiva percorribile per ricavare nuovi elementi di conoscenza non noti a priori contenuti nei dati e nelle informazioni raccolte*» [27].

Maturate tali consapevolezze, non va nondimeno sottaciuto come l'indubbia rilevanza strategica apportata dai nuovi strumenti in commento nel contesto investigativo non appaia comunque esente da possibili criticità.

Fermo restando quanto già osservato in dottrina con riferimento allo specifi-

scute in merito alla possibilità di impiegare di sistemi di IA, è quello concernente la valutazione della pericolosità sociale e criminale degli individui, cui è necessario procedere laddove si riveli necessario applicare una misura di prevenzione, di sicurezza, una misura cautelare o anche ad altri fini. In tale contesto, si prevede la possibilità di affidare in futuro le valutazioni prognostiche di pericolosità sociale ad appositi algoritmi predittivi, i cd. *risk assessment tools*, in grado di ricavare e rielaborare ingenti quantità di dati con lo scopo di far emergere relazioni o coincidenze che consentano di tracciare il profilo di un individuo e prevederne i successivi comportamenti, anche di rilevanza penale. Infine, altro coinvolgimento dell'intelligenza artificiale nel campo del diritto penale è rinvenibile con riferimento ai possibili rapporti della macchina con il reato, in merito cioè alla possibilità di configurare la stessa come strumento, autore o vittima dell'illecito penale. Per una disamina dettagliata sulle questioni qui brevemente richiamate, v. F. BASILE, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, cit., p. 14 ss., in cui l'A. si sofferma diffusamente su tutti i possibili ambiti applicativi sopra menzionati; G. RICCIO, *Ragionando su intelligenza artificiale e processo penale*, in *Arch. pen*., 3, 2019; G. UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, cit.; G. PADUA, *Intelligenza artificiale e giudizio penale: scenari, limiti e prospettive*, in *www.processopenaleegiustizia.it*; e A.M. MAUGERI, *L'uso di algoritmi predittivi per accertare la pericolosità sociale: una sfida tra evidence based practices e tutela dei diritti fondamentali*, in *Arch. pen*., 1, 2021, ove l'A. analizza in chiave problematica le prospettive legate all'utilizzo di algoritmi predittivi per valutare la pericolosità sociale degli individui. Con riferimento invece al possibile impiego dell'intelligenza artificiale in ambiti ulteriori ed estranei a quelli strettamente penalistici, quale ad esempio quello pubblicistico, v. D. MARONGIU, *L'intelligenza artificiale "istituzionale": limiti (attuali) e potenzialità*, in *Eur. Rev. of Digital. Admin. & Law*, Erdal, 1, 1-2, 2020, *The Use of AI by Public Administration*, pp. 37-53.

[26] V. *supra*, § 1, nota 17.

[27] Così evidenziato in *L'impatto dell'Intelligenza Artificiale sul ciclo di intelligence e sugli strumenti a disposizione per i pianificatori militari e le forze dell'ordine*, cit., p. 69 ss.

co problema del rapporto intercorrente tra raccolta e utilizzo dei dati di carattere personale e tutela delle garanzie individuali [28], ad una ulteriore riflessione induce proprio la principale caratteristica di siffatti sistemi, ossia la capacità di estrarre dalle risorse a disposizione dati e informazioni in grado di rivelare conoscenze e suggerire indizi di interesse investigativo.

Tale capacità postula, necessariamente, un'adeguata organizzazione e un attento coordinamento, costituendo siffatti dati elementi di conoscenza di valore centrale poiché scrigno di notizie inedite, talvolta di natura strettamente personale, la cui condivisione e il cui trattamento vanno adeguatamente circoscritti.

Nel contempo, gli stessi devono poter essere facilmente accessibili da parte degli operatori legittimati, ma anche archiviati, elaborati e agevolmente disponibili per il riuso.

Se il problema appare meno spinoso con riferimento al settore "privato", altrettanto non sembra potersi affermare, ad esempio, relativamente all'ambito governativo cui le attività di polizia spesso afferiscono, posto che, in tale contesto, i dati risultano di interesse collettivo in quanto strettamente connessi alla sicurezza nazionale.

Assume quindi fondamentale rilievo il delicato compito di raccolta dei dati e delle informazioni per finalità investigative. In tale ottica, l'organizzazione necessaria per l'approccio alle *big data analytics* richiede adeguata maturità e, come già evidenziato, un attento coordinamento.

Alla luce di quanto emerso dalla presente ricerca e dalle considerazioni sin qui svolte, è dunque possibile trarre alcune brevi conclusioni.

È da porre in rilievo come le strumentazioni e le metodologie esaminate, sebbene rappresentino già allo stato attuale elementi di grande novità e di notevole impatto sulle attività investigative, racchiudano in sé enormi prospettive di crescita e di sviluppo, destinate indubbiamente ad evolversi e perfezionarsi ulteriormente nel prossimo futuro.

Particolare attenzione dovrà essere posta, a parere di chi scrive, in una duplice prospettiva. Da un lato, adottando un'adeguata organizzazione che tenga conto della centralità dei dati nel funzionamento di questo nuovo sistema che potremmo definire, per l'appunto, "data-centrico", affinché gli stessi possano essere trattati, elaborati e analizzati con una precisione e una sicurezza progressivamente accresciute.

In secondo luogo, curando adeguatamente la formazione e il costante aggior-

[28] G. UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, cit., pp. 79-80, ove l'A. rileva come in materia emerga, in tutta la sua importanza, il fondamentale tema delle garanzie individuali, da osservare a partire dal momento della raccolta dei dati di carattere personale fino all'utilizzo dei risultati della loro elaborazione. Per ulteriori approfondimenti, si rinvia a tal sede.

namento di figure professionali specificamente competenti per il trattamento, la gestione e la raccolta dei suddetti dati.

Ad ogni modo, il futuro e certo evolversi dei sistemi basati sull'intelligenza artificiale, anche con riguardo all'attività investigativa propria delle forze dell'ordine, non sarà esente da possibili rischi, ma si tratta di una sfida da raccogliere con coraggio, da affrontare e superare con la necessaria competenza e con attenzione costante.

CAPITOLO IX

Sicurezza alimentare e nuove tecnologie. I possibili scenari di un rapporto ambiguo

GIUSEPPE ALESCI

SOMMARIO: 9.1. Introduzione. – 9.2. Sicurezza alimentare e nuove tecnologie. – 9.3. L'inadeguatezza del tradizionale modello punitivo delle frodi alimentari. – 9.4. I margini di applicabilità delle nuove tecnologie nel diritto penale agro-alimentare. – 9.5. Ridurre per adeguare; semplificare per rinnovare. – 9.6. Conclusioni.

9.1. *Introduzione*

Parole come *Blockchain*, *Smart Contracts*, *Internet delle cose*, *Big Data*, *QR Code*, *RFID*, *e-commerce*, *Intelligenza Artificiale* sono ormai parte del lessico tanto comune quanto giuridico. «*Ce le ritroveremo dappertutto*» [1], è stato detto, e così è stato, anche nel settore agroalimentare. In questo contesto, in particolare, l'impiego delle nuove tecnologie ha avuto un impatto molto invasivo all'interno della filiera, investendo sia i processi di produzione e distribuzione dei prodotti sia la sperimentazione genetica degli alimenti. La recente crisi pandemica, peraltro, con l'adozione delle necessarie misure di contenimento, ha accelerato la diffusione di nuovi strumenti tecnologici, (ab-) usati tanto ai fini dell'approvvigionamento quanto della distribuzione dei prodotti, soprattutto di prima necessità.

In questa mutata realtà fenomenica, la regolamentazione della materia, ormai obsoleta, necessita, più che di un mero aggiornamento, di un profondo ripensamento dell'originario impianto sanzionatorio. L'applicazione delle nuove tecnologie in un settore così suscettibile alle oscillazioni del mercato, infatti, se non bilanciata con attenzione, può sì rappresentare un beneficio in termini di *food*

[1] M.A. BODEN, *Intelligenza artificiale*, in J. AL-KHALILI (a cura di), *Il futuro che verrà*, Bollati Boringhieri, Torino, 2018, p. 133.

security, ma anche un pericolo in termini di *food safety*[2]. Se da un lato, cioè, l'impiego di queste nuove risorse favorisce l'accesso al cibo sostenibile anche attraverso la creazione di nuovi prodotti nati da modelli di *machine learning,* con un apparente miglioramento della qualità del prodotto, dall'altro insinua forme di aggressione alla sicurezza alimentare dapprima impensabili, che coinvolgono profili tra loro eterogenei: dalle molteplici modalità di frodi dei prodotti nell'*e-commerce* ai nuovi pericoli derivanti dalle manipolazioni genetiche.

Nondimeno, questo accade se l'impiego delle nuove tecnologie non viene attentamente regolamentato dal legislatore, il quale, al contrario, potrebbe servirsene in funzione di *law enforcement*, ovvero per rafforzare gli attuali strumenti di prevenzione degli illeciti. Il riferimento, a titolo esemplificativo, è all'applicabilità agli alimenti del *fingerprinting* (la cd. impronta digitale) metabolomico che, se è affiancato ad un robusto sistema di certificazioni adeguatamente disciplinato, ovvero la *blockchain*, può costituire un valido strumento di prevenzione della sicurezza alimentare. La loro efficace applicazione comporta, tuttavia, un'anticipazione della tutela ragionata su una nuova logica di tipo precauzionale, che può essere meglio assicurata soltanto attraverso un rovesciamento dell'attuale schema punitivo.

Il presente contributo si propone, pertanto, di illustrare, senza alcuna pretesa di esaustività, tali profili, indicando i problemi e le prospettive connessi all'impiego delle innovazioni nel diritto penale agroalimentare, con l'obiettivo di esaminare luci e ombre di un rapporto evidentemente ambiguo, in cui la novità tecnologica può costituire uno strumento di tutela della sicurezza alimentare ma al tempo stesso, se non adeguatamente presidiata, anche di offesa.

9.2. *Sicurezza alimentare e nuove tecnologie*

Il mercato delle frodi alimentari è indubbiamente in forte crescita e le periodiche inchieste giudiziarie ne sono la conferma[3]. Tra le principali ragioni della

[2] I concetti appena richiamati non devono essere confusi. La cd. *food security*, infatti, è intesa come diritto al cibo o, meglio, come «la garanzia di un accesso fisico, economico e sociale a un'alimentazione sufficiente, sicura e nutritiva, adeguata a tutti, e dunque quale disponibilità dell'uomo agli approvvigionamenti alimentari minimi per soddisfare il suo bisogno naturale ed irrinunciabile»; la *food safety*, invece, ha una sua dimensione giuridica, da intendersi (per quanto genericamente) come sicurezza dei prodotti alimentari rispetto alla loro produzione, manipolazione, preparazione e conservazione (ovvero sicurezza alimentare). Nondimeno, ricondotti alle coordinate che qui più direttamente rilevano, *security* e *safety* convergono reciprocamente, costituendo l'uno la premessa dell'altro. Per un approfondimento sul punto, volendo, si v. G. ALESCI, Fake foods e novel foods. *La sicurezza alimentare tra vecchie criticità e nuove prospettive*, in *Leg. pen*., 12 aprile 2022.

[3] Risale al giugno 2021 la notizia di un maxi sequestro presso un'azienda dell'Agro No-

diffusione del fenomeno incide notevolmente la caotica disciplina della materia. I molteplici interessi coinvolti, dalla salute pubblica all'economia pubblica, dalla lealtà commerciale dei produttori alla corretta informazione dei consumatori, da un lato, e la sensibilità verso i mutevoli postulati della scienza, dall'altro, rendono fragile ed estemporanea la regolamentazione, pregiudicando inevitabilmente la conoscibilità dei precetti, la coerenza del sistema e la tenuta empirica delle fattispecie. L'apparente assenza di una riconoscibile razionalità politico-criminale delle prescrizioni, peraltro ramificate in ogni dove, tanto nel diritto penale quanto in quello civile e amministrativo, deve attribuirsi anche all'intreccio di normative di epoche differenti, che nel tentativo di adeguare la disciplina ai nuovi pericoli del mercato si sono succedute senza un'ossatura comune [4].

In un panorama così vasto e naturalmente complesso, l'utilizzo delle nuove tecnologie per la produzione, il controllo e la distribuzione dei prodotti agroalimentari, se non attentamente regolato, rischia di compromettere integralmente la tenuta prescrittiva del sistema, con inevitabili ricadute sul futuro della sicurezza alimentare [5], esposta a forme di aggressione sempre più insidiose e dapprima impensabili.

cerino Sarnese, leader nel settore conserviero, di una partita di ben 821 tonnellate di concentrato di pomodoro di provenienza egiziana, del valore di circa un milione di euro, risultato contaminato da pesticidi, presenti in misura maggiore a quanto normativamente consentito, sussistendo così il concreto rischio di nocività per la salute umana. L'operazione "Scarlatto Due", condotta dalla Procura della Repubblica di Nocera Inferiore, segue di poche settimane un'altra significativa attività investigativa (operazione "Scarlatto"), che ha visto il sequestro di migliaia di tonnellate di concentrato di pomodoro di provenienza estera, fraudolentemente inserito nel ciclo produttivo per realizzare conserve alimentari illecitamente commercializzate come "pomodoro 100% toscano". Per la Coldiretti, il sequestro, in una zona tradizionale di produzione come la Campania, conferma l'allarme per l'aumento delle importazioni in Italia di derivati di pomodoro del 23% nel primo bimestre del 2021 soprattutto dalla Cina con quantitativi che sono però praticamente raddoppiati dall'Egitto (+83%) rispetto allo scorso anno. Fonte tratta dal quotidiano *online "Italia a Tavola"*, 8 giugno 2021.

[4] Per una veloce panoramica della complessità della stratificazione del diritto alimentare, costituita da fonti di ogni ordine e grado (internazionali, europee e nazionali, di *hard law* quanto di *soft law*), si veda D. CASTRONUOVO, *Sicurezza alimentare*, in M. DONINI, D. CASTRONUOVO (a cura di), *La riforma dei reati contro la salute pubblica. Sicurezza del lavoro, sicurezza alimentare, sicurezza dei prodotti*, Cedam, Padova, 2007, p. 22; o ancora, A. BERNARDI, *Il processo di razionalizzazione del sistema sanzionatorio alimentare tra codice e leggi speciali*, in *Riv. trim. dir. pen. econ.*, 2002, p. 67; più di recente, fra gli altri, A. GARGANI, *Reati contro l'incolumità pubblica*, tomo II, Giuffrè, Milano, 2013, p. 248 ss.

[5] Affermatasi con prepotenza come nuovo bene giuridico, figlia della modernità e dell'evoluzione scientifica, la sicurezza alimentare si presenta oggi come eterogenea, polimorfica e dal contenuto ancora sfuggente, prospettando di sé diverse definizioni. Comunemente identificata con la cd. *food security*, intesa come diritto al cibo o, meglio, come «la garanzia di un

Si pensi, a titolo esemplificativo, all'*e-commerce*[6]. È proprio in questo mercato – peraltro cresciuto nell'ultimo periodo del +117% nel settore del largo consumo, con incrementi maggiori proprio durante il recente periodo di pandemia[7] – che si annida il timore di incorrere in nuove forme di frodi alimentari. Le ragioni sono evidentemente molteplici e riguardano la facilità con cui il prodotto alimentare, nel commercio *on-line*, potrebbe subire contraffazioni in termini soprattutto di qualità, salubrità e igiene: dalla facile deperibilità del prodotto, se non stoccato o trasportato in regime di temperatura controllata, alla mancanza della tracciabilità e rintracciabilità dello stesso, di cui è conosciuto – e peraltro non sempre – solo il distributore (cioè il rivenditore *on-line*). Ciò, nonostante le precauzioni imposte in capo al proprietario del sito *web* dal Regolamento 2011/1169/UE che, al-

accesso fisico, economico e sociale a un'alimentazione sufficiente, sicura e nutritiva, adeguata a tutti, e dunque quale disponibilità dell'uomo agli approvvigionamenti alimentari minimi per soddisfare il suo bisogno naturale ed irrinunciabile», la sicurezza alimentare, nella sua dimensione giuridica, va invece qualificata come *food safety*, da intendersi (per quanto genericamente) come sicurezza dei prodotti alimentari rispetto alla loro produzione, manipolazione, preparazione e conservazione. Nondimeno, ricondotto alle coordinate che qui più direttamente rilevano, appare chiara la relazione con il bene della "salute", tanto individuale quanto collettiva, di cui appare costituire un predicato in cui *security* e *safety* convergono reciprocamente, costituendo l'uno la premessa dell'altro. La sicurezza alimentare costituisce, dunque, un bene dalla titolarità nel contempo individuale e diffusa, mostrando una bipolarità teleologica che lo qualifica come bene intermedio, di categoria, a carattere strumentale, ponendosi tra la sfera di tutela della salute pubblica e lo scopo ultimo della tutela stessa. Ecco, allora, che «i reati specificamente agroalimentari costituiscono un nucleo importante, non separabile concettualmente, ma in parte solo geograficamente, dalla restante disciplina della salute». Cfr., *ex multis*, M. RAMAJOLI, *Dalla "food safety" alla "food security" e ritorno*, in *Amministrare*, 2015, pp. 271-92; A. GARGANI, *Il pericolo comune e la nozione di disastro sanitario nel settore alimentare: profili* de lege ferenda, in L. FOFFANI, A. DOVAL PAIS, D. CASTRONUOVO (a cura di), *La sicurezza agroalimentare nella prospettiva europea. Precauzione, prevenzione e repressione*, Giuffrè, Milano, 2014; M. DONINI, *Il progetto del 2015 della Commissione Caselli*, in *Dir. pen. cont*., 1, 2016, pp. 5-30; si veda anche ID., *Il progetto di riforma dei reati in materia di sicurezza alimentare*, in *Cass. pen*., 12, 2010, p. 4463 ss.

[6] Rinviando ad altre sedi più opportune una più puntuale definizione, l'*e-commerce* può genericamente definirsi come l'insieme delle transazioni commerciali effettuate via Internet. Tale definizione è però riduttiva dal momento che l'*e-commerce* non si esaurisce nella semplice transazione, ma può abbracciare anche altre fasi e aspetti della relazione negoziale tra produttore (offerta) e consumatore (domanda). L'*e-commerce*, infatti, concerne anche tutte le relazioni commerciali, realizzate mediante l'uso di computer e reti telematiche, che sono volte allo scambio di informazioni direttamente correlate alla vendita di beni e servizi.

[7] I dati statistici, d'altronde, confermano che l'*e-commerce* del *food* è stato uno dei comparti con maggiore incrementi durante l'anno 0 della pandemia, con un tasso di crescita molto più alto della media (+70% rispetto al 2019) e un valore di 2,7 mld €. Dati tratti da *Osservatori.net*, 1 febbraio 2021.

l'art. 14 dedicato alla *vendita a distanza di alimenti*, prevede una serie di prescrizioni da adempiere relative alle informazioni obbligatorie del prodotto in vendita [8].

In un mercato con queste dinamiche, l'individuazione della corretta provenienza dei prodotti alimentari, del loro confezionamento, della loro successiva distribuzione diventa particolarmente faticosa; altrettanto in termini di accertamento delle responsabilità, che si snodano tra i vari attori dell'intricata filiera. Peraltro, la velocità con cui il prodotto giunge dal campo alla tavola ne impedisce un adeguato controllo, con il rischio di rilevare la contraffazione soltanto quando ormai è stato già venduto o consumato.

Medesime preoccupazioni riguardano anche i cd. *OGM* [9]. L'applicazione di biotecnologie sperimentali nella produzione di alimenti creati in "laboratorio", infatti, amplifica le probabilità di immettere sul mercato prodotti pericolosi [10].

[8] Trattasi, peraltro, di una disposizione preponderante rispetto a quelle riportate nel d.lgs. n. 21/2014 (recepimento della Direttiva "Consumatori" 2011/83/UE) anche se introdotte nel Codice del Consumo grazie al fatto che la citata direttiva prevedeva (art. 3 e considerando 11) che «(…) le comunicazioni elettroniche (…) l'etichettatura dei prodotti alimentari (…) sono lasciate impregiudicate». Secondo la vigente normativa, per i *Prodotti alimentari preimballati* le principali informazioni obbligatorie sono: la denominazione dell'alimento; l'elenco degli ingredienti; l'elenco degli allergeni presenti; le dichiarazioni nutrizionali; la quantità netta; la ragione sociale o nome e l'indirizzo dell'OSA (Operatore del settore alimentare) che commercializza il prodotto [costui rappresenta il responsabile]; le particolari condizioni di impiego e/o di conservazione; le eventuali istruzioni per l'uso qualora queste, se mancanti, non permettono il corretto uso dell'alimento; il Paese d'origine o luogo di provenienza; il titolo alcolimetrico volumico effettivo per le bevande che contengono più del una percentuale di alcol superiore a 1,2% in volume.

[9] Con la sigla *OGM* si fa riferimento a «un organismo, diverso da un essere umano, il cui materiale genetico è stato modificato in modo diverso da quanto si verifica in natura mediante accoppiamento o incrocio o con la ricombinazione genetica naturale». Così l'art. 3, comma 1, lett. b), d.lgs. n. 224/2003 (*Attuazione della dir. 2001/18/CE concernente l'emissione deliberata nell'ambiente di organismi geneticamente modificati*). Per una compiuta disamina dei problematici profili giuridici, cfr. F. CONSORTE, *L'intervento penale nel settore degli organismi geneticamente modificati (OGM). Il ruolo del principio di precauzione*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Trattato di diritto penale* (a cura di), *Parte speciale*, vol. IV, *I delitti contro l'incolumità pubblica e in materia di stupefacenti*, Utet, Torino, 2010, p. 475 ss.

[10] L'impiego di OGM nel settore alimentare divide non solo l'opinione pubblica ma anche la scienza. Da una parte si collocano coloro i quali sostengono che le piante geneticamente modificate siano sicure e rappresentino un'occasione per produrre più cibo, a prezzi più bassi, e con maggiore rispetto per l'ambiente; dall'altro, invece, ci sono coloro i quali ritengono che gli *OGM* siano il «cibo di *Frankestein*», un espediente delle multinazionali per lucrare quanto più possibile, a scapito della salute dei consumatori, dell'equilibrio dell'ecosistema, della biodiversità, e dell'economia dei Paesi più poveri. Cfr. L. TUMMINELLO, *Sicu-*

Le numerose precauzioni adottate nel corso del recente passato dal legislatore, dalla previsione di stringenti autorizzazioni amministrative alle rigide regole di etichettatura, non escludono infatti il rischio di una loro arbitraria manipolazione, che può esporre la sicurezza alimentare – soprattutto, in questo caso, in termini di nocività – a nuovi rischi («da ignoto biotecnologico») non preveduti né adeguatamente prevenuti [11].

Se tuttavia le nuove tecnologie possono rappresentare un *input* per la diffusione di condotte fraudolente dapprima impensabili o comunque meno diffuse, nondimeno possono porsi anche come strumento di contrasto e, soprattutto, di prevenzione alle multiformi modalità di illeciti che si celano praticamente in ogni dove della filiera. L'uso di metodi innovativi, rapidi e affidabili, offerti dalla tecnologia – dalla *blockchain* come nuovo strumento di tracciabilità del prodotto all'impiego di etichette con codici *QR*, o ancora agli strumenti di impronta digitale degli alimenti (cd. *fingerprinting*) –, se adeguatamente applicate, possono infatti rappresentare una valida opzione per migliorare la qualità della tutela della sicurezza alimentare.

Si tratta tuttavia di temi ancora poco scrutinati, sia sul piano della loro certezza scientifica – il riferimento è soprattutto alle loro diverse modalità di applicazione –, sia su quello della regolamentazione giuridica. In questo senso, si rivela indispensabile un ripensamento dell'attuale modello di disciplina della materia e, in particolare – per il profilo che qui interessa – di prevenzione degli illeciti, attraverso una riforma che, in una prospettiva di riduzione e semplificazione della precettistica, si confronti con la modernità individuando soluzioni appropriate.

rezza alimentare e diritto penale: vecchi e nuovi paradigmi tra prevenzione e precauzione, in *Dir. pen. cont*., 4, 2013, p. 300 ss.; cfr. F. SALA, *Gli OGM sono davvero pericolosi?,* II ed., Laterza, Roma-Bari, 2005, p. 5 ss.

[11] Si pensi alla possibile trasmissione dei geni resistenti agli antibiotici dagli *OGM* all'uomo, l'istaurarsi di reazioni allergiche dovute al consumo di tali prodotti, o ancora al caso della soia modificata con i geni della noce brasiliana, e l'instaurarsi di effetti tossici che potrebbero sviluppare, soprattutto nel medio e lungo periodo, nell'organismo umano. Si rinvia per un approfondimento a S. CORBETTA, *Sicurezza alimentare e rischio da "ignoto tecnologico": una tutela incompiuta*, *(a proposito della disciplina degli alimenti e dei mangimi contenenti organismi geneticamente modificati – d.lgs. 21 marzo 2005, n. 70)*, in E. DOLCINI, C.E. PALIERO (a cura di), *Studi in onore di G. Marinucci*, Giuffrè, Milano, 2006, pp. 2257-301; D. CASTRONUOVO, *Principio di precauzione e beni legati alla sicurezza*, in *www.diritto penalecontemporaneo.it*, 21 luglio 2011, 17.

9.3. *L'inadeguatezza del tradizionale modello punitivo delle frodi alimentari*

L'applicazione delle nuove tecnologie ha pervaso qualsiasi settore della delinquenza: dalla produzione, distribuzione e traffico di droghe sintetiche al traffico di migranti, dal riciclaggio di denaro sporco al commercio *online* di prodotti e servizi illegali. La versatilità della modernità di insinuarsi nelle logiche criminali, d'altronde, favorisce nuove opportunità di illeciti, e questo è accaduto anche – ma soprattutto – con riguardo al settore agro-alimentare.

L'inestricabile complessità della materia, infatti, ha da sempre compromesso la rigidità strutturale del tipo di illecito – comunemente identificato nella frode alimentare –, ciò consentendo che nel tempo si avviluppassero eterogenee forme di aggressioni difficili da classificare e tipizzare. Ed infatti, nonostante sia una delle attività criminose più antiche e saldamente radicate nella vita sociale dai tempi della Bibbia [12], la flessibilità delle condotte non ha mai permesso l'individuazione di una sua precisa identità illecita, se non approssimando una catalogazione della tipologia dell'illecito esclusivamente in relazione al bene offeso dalla condotta. La più generica frode alimentare è stata così distinta in sanitaria e commerciale: la prima abbraccia tutte le ipotesi in cui la manipolazione del prodotto espone al pericolo o lede la salute del consumatore; la seconda, invece, comprende tutte quelle condotte che, non determinando un concreto o immediato pericolo per la salute pubblica, favoriscono illeciti profitti a danno di terzi o del consumatore. Tuttavia, rinvenire questa distinzione nella quotidianità non è così immediata, soprattutto perché la varietà casistica, peraltro spesso episodica, coinvolge numerosi profili variabili per le differenti modalità di aggressione o per le molteplici proprietà del prodotto che possono essere compromesse. Si va, a titolo esemplificativo, dall'adulterazione (si pensi al vino al metanolo per aumentarne la gradazione) alla sofisticazione (è il caso della mozzarella al perossido di benzoile con effetto sbiancante), dall'alterazione (i vini fermentati con invertasi, o mozzarella prodotta con caseina) alla contraffazione (margarina proveniente da grassi minerali); così come la manipolazione del prodotto può incidere sul tasso di nocività [13] anziché sulla tossicità, sulla con-

[12] Per un interessante spaccato della storia delle frodi alimentari, dalle origini sino all'età moderna, si rinvia alla lettura di G. NEBBIA, G. MENOZZI NEBBIA, *Breve storia delle frodi alimentari*, in S. CANEPARI, C. MALTONI, F. SACCANI (a cura di), *Alimentazione e salute*, Monduzzi, Forlì, 1986, pp. 60-8; si veda anche G. STEA, *Elementi per un'analisi del reato alimentare tra rischio, pericolo e necessità di prevenzione*, in *Riv. dir. alim.*, 2, 2018, pp. 42-71.

[13] La nocività di cui all'art. 444 c.p. consiste nell'attitudine che ha una sostanza alimentare di creare un danno alla salute del consumatore. In questo caso, la pericolosità non è data

formità e, in particolare, sulla genuinità [14] ma anche sullo stato di conservazione o sul confezionamento [15].

Eppure, nonostante questa inestricabile complessità della materia costituisca un tangibile limite alla predisposizione di una disciplina realmente capace di assolvere una funzione preventiva, il legislatore è nel tempo riuscito (a fatica) a predisporre un modello sanzionatorio dosimetrico, comunemente riassunto in tre livelli, che accoglie illeciti sia amministrativi, sia contravvenzionali, nonché ipotesi delittuose [16].

dall'astratta e ipotetica possibilità di arrecare nocumento, ma dall'attitudine concreta del prodotto di provocare un danno alla salute se consumato nello stato in cui si trova.

[14] La genuinità è tradizionalmente distinta in due categorie: naturale e formale. La prima è circoscritta alle sostanze che non abbiano subito alterazioni né modificazioni da parte dell'uomo, comprendendo, altresì, i casi in cui la manipolazione non si sia avuta per mezzo di elementi chimici, quanto tramite componenti naturali della sostanza stessa, utilizzati in maniera abnorme. La seconda, invece, rappresenta il parametro secondo cui si afferma la corrispondenza della sostanza alimentare con le varie prescrizioni legislative in merito. In tal caso, il reato potrà, ad esempio, essere commesso nel caso di prodotti contenenti sostanze diverse da quella indicate *ex lege* per la loro composizione, oppure che contengono sostanze di per sé genuine, ma che risultano essere presenti in misura superiore o inferiore a quella consentita, tenendo comunque a mente che non è richiesta una messa in pericolo dell'incolumità pubblica ai fini dell'integrazione della fattispecie. La casistica offre vari esempi di non genuinità formale, come nel caso del "grana padano" confezionato con latte termizzato, vietato dalle disposizioni che regolano la denominazione d'origine del prodotto, oppure la messa in commercio di pane con all'interno quantitativi di acqua superiori al massimo consentito.

[15] Per un approfondimento, anche contenutistico, delle diverse condotte fraudolente di manipolazione dei prodotti agroalimentari, si rinvia a S. MASINI, *Corso di Diritto Alimentare*, V ed., Giuffrè, Milano, 2020, e, per una disamina datata ma quanto mai attuale delle stesse, F. BRICOLA, *Tipologia delle frodi nella normativa penale sugli alimenti*, in S. CANESTRARI, A. MELCHIONDA (a cura di), *F. Bricola. Scritti di diritto penale*, vol. II, *Parte Speciale e legislazione complementare. Diritto penale dell'economia*, tomo I, Giuffrè, Milano, 1997, p. 2420 ss.

[16] La classificazione "su tre livelli" della disciplina in materia alimentare è ormai una costante della dottrina più notevole, cui si rinvia per un approfondimento. Tra gli altri, cfr. A. BERNARDI, *Il processo di razionalizzazione del sistema alimentare*, cit., p. 64; D. CASTRONUOVO, *Depenalizzazione e modelli di riforma penale: il "paradigma" del sistema di illeciti in materia penale*, in *Ind. pen*., 2001, p. 303; A. GARGANI, *Reati contro l'incolumità pubblica*, tomo II, *Reati di comune pericolo mediante frode*, in C. GROSSO, T. PADOVANI, A. PAGLIARO (diretto da), *Trattato di diritto penale. Parte speciale*, Giuffrè, Milano, 2013, p. 273 ss.; ancora, S. CORBETTA*, I delitti contro l'incolumità pubblica. I delitti di comune pericolo mediante frode*, in G. MARINUCCI, E. DOLCINI (diretto da), *Trattato di diritto penale. Parte speciale,* tomo II, Cedam, Padova, 2014, p. 124 ss. La "tripartizione" è stata più di recente ripresa da L. TUMMINELLO, *Sicurezza alimentare e diritto penale*, cit., p. 272 ss.; G. TOSCANO, *Bene giuridico e modelli di tutela nella disciplina degli illeciti alimentari: riflessioni de iure condendo (anche) nella prospettiva della riserva di codice*, in *www.legislazionepenale*

Molto brevemente: al ginepraio di sanzioni amministrative relative prevalentemente alle violazioni di prescrizioni commerciali o in materia di imballaggio [17], si affiancano le più diffuse fattispecie contravvenzionali previste dalla l. 30 aprile 1962, n. 283 relativa alla «disciplina igienica della produzione e della vendita delle sostanze alimentari e delle bevande». In particolare, secondo quanto previsto dall'art. 5, è vietato impiegare nella preparazione di alimenti o bevande, vendere, detenere per vendere o somministrare come mercede ai propri dipendenti, o comunque distribuire per il consumo, sostanze alimentari non conformi sotto il profilo dell'igiene, genuinità e purezza e, in generale, la sicurezza delle stesse [18]. Vi sono poi le fattispecie identificate propriamente come delittuose dal codice penale. Dapprima, infatti, sono elencate le ipotesi di cui agli

.eu, 4 febbraio 2019, p. 11 ss. Per una visione parzialmente diversa, preferendo uno schema "pentapartito" dei modelli di tutela esistenti e *in fieri* nel diritto penale alimentare, v. M. DONINI, *La riforma dei reati alimentari: dalla precauzione ai disastri. Per una modellistica pentapartita degli illeciti in materia di salute e sicurezza alimentare*, in B. BISCOTTI, E. LAMARQUE (a cura di), *Cibo e acqua. Sfide per il diritto contemporaneo. Verso e oltre expo 2015*, Giappichelli, Torino, 2015, pp. 21-45; o, ancora, ID., *Il progetto 2015 della Commissione Caselli*, in *Riv. trim. dir. pen. cont*., 1, 2016, pp. 4-30. L'A., infatti, ritiene più corretto individuare cinque modelli di intervento legislativo: 1) un modello precauzionale puro, che oscilla tra il diritto penale e quello amministrativo, tipico ad esempio degli *OGM*; 2) un modello di tutela amministrativa classica, caratterizzato da ipotesi minori di pericolo astratto-presunto o di rischio; 3) un modello propriamente contravvenzionale; 4) un modello codicistico riservato ai delitti contro la salute pubblica; 5) un modello-residuale, a tutela dell'integrità individuale e della vita.

[17] Ad oggi gli illeciti amministrativi alimentari, registrati dal sistema informativo dell'ICQRF, cioè l'Ispettorato centrale per la tutela della qualità e la repressione delle frodi presso il Ministero delle politiche agricole e forestali, sono circa un migliaio. Cfr. R. MIRABELLI, *Il ruolo del Ministero della salute nell'attuazione delle norme in materia di sicurezza alimentare*, in C. BOTTARI (a cura di), *La sicurezza alimentare. Profili normativi e giurisprudenziali tra diritto interno, internazionale*, *ed europeo*, Maggioli, Santarcangelo di Romagna, 2015, p. 45 ss. La maggior parte della pletora di illeciti amministrativi provengono tanto da numerose leggi speciali quanto dai decreti attuativi della abbondante e recente opera di regolazione sovranazionale, da cui ad ultimo il Regolamento 625/2017/UE. Per un approfondimento, cfr. L. CARRARA, *Dal Regolamento (UE) 2017/625 alle misure applicative unionali e nazionali: un percorso innovativo ma non concluso*, in *Riv. dir. alim.,* 4, 2020, pp. 37-47; ancora, F. ALBISINNI, *Il Regolamento (UE) 2017/625: controlli ufficiali, ciclo della vita, impresa e globalizzazione*, in *Riv. dir. alim*., 1, 2018, pp. 11-36.

[18] Per un'approfondita disamina delle fattispecie contravvenzionali qui soltanto richiamate per brevità, si veda V. PACILEO, *Il diritto degli alimenti. Profili civili, penali e amministrativi*, Cedam, Padova, 2003, p. 51; C. CORRERA, *Tutela igienico-sanitaria degli alimenti e bevande*, Giuffrè, Milano, 1991, p. 1107; R. FRESA, *Le fattispecie contravvenzionali della l. 283/1962 (artt. 5, 6, 12*), in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (a cura di), *Trattato di diritto penale*, cit., p. 436.

artt. 439, 440, 442, 444 c.p., ovvero, sinteticamente, le condotte di avvelenamento, adulterazione o contraffazione di sostanze alimentari e il loro commercio, anche se nocive [19]; e successivamente, le ipotesi previste invece dagli artt. 515, 516 e 517 c.p. [20], propriamente dirette alla tutela dell'economia pubblica e, in particolare, della buona fede negli scambi commerciali. In questo caso, infatti, l'azione fraudolenta sull'alimento o sulla sua confezione, pur non determinando un concreto o immediato nocumento per la salute pubblica, favorisce illeciti profitti sia a danno del consumatore sia del produttore o del commerciante, nei cui confronti si realizzerebbe una concorrenza sleale.

L'apparente semplicità di questo schema, tuttavia, non riflette la concreta difficoltà operativa di rintracciare nella quotidianità la corrispondenza tra il fatto compiuto e quello tipizzato dalla norma. Una difficoltà, peraltro, non solo riconducibile alla naturale variabilità della casistica empirica, ma anche alla complessità intrinseca della regolamentazione, nella quale si accavallano snodi disciplinari e polimorfismi lessicali che disorientano l'interprete nel momento applicativo [21]. La responsabilità è certamente da attribuirsi anche agli affanni del legislatore, il quale negli anni ha colmato gli emergenti e costanti vuoti di tutela attraverso frammentari quanto maldestri interventi, disinteressandosi completamente degli effetti pratici della propria confusione. Ciò si è chiaramente riverberato sull'ossatura dell'originario modello disciplinare, che si è così indebolito e mostrato inadeguato ad accogliere le nuove (e multiformi) identità degli illeciti.

Anche per questi motivi, d'altronde, sono circa vent'anni che si ragiona intorno ad una riforma radicale della materia, volta da un lato a razionalizzarne gli

[19] Più precisamente, si tratta delle fattispecie di cui al Capo II (Dei delitti di comune pericolo mediante frode), Titolo VI (Dei delitti contro l'incolumità pubblica), che sanzionano l'avvelenamento di acque e di sostanze alimentari (art. 439 c.p.), l'adulterazione o contraffazione di sostanze alimentari (art. 440 c.p.), il commercio di sostanze alimentari contraffatte o adulterate (art. 442 c.p.), e il commercio di sostanze alimentari nocive (art. 444 c.p.). Si tende ad identificare queste ipotesi nella cd. "frode sanitaria".

[20] Esattamente, il rinvio è all'art. 515 c.p., rubricato "Frode nell'esercizio del commercio", art. 516 c.p., rubricato "Vendita di sostanze alimentari non genuine come genuine" e, infine, art. 517 c.p., "Vendita di prodotti industriali con segni mendaci".

[21] Secondo G. PICA, voce *Illeciti alimentari*, in *Enc. dir*., VI ed., Giuffrè, Milano, 2002, p. 444 ss., il polimorfismo lessicale è proprio delle diverse ipotesi tipizzate nel tempo: nocività, tossicità, conformità, genuinità; o ancora, avvelenamento, adulterazione, sofisticazione, contraffazione, alterazione, corrompimento, additivazione, contaminazione, stato di conservazione degli alimenti e delle bevande, delle sostanze alimentari, dei prodotti alimentari, delle sostanze destinate all'alimentazione. Tutto ciò genera inevitabilmente una grande confusione tra ipotesi molto diverse: dalla genuinità (che è un problema di frode commerciale) alla salute, alle inosservanze di regole di autorizzazione o di limiti – soglia sino alla preparazione, ma anche alla vendita di sostanze nocive.

aspetti multidisciplinari e, dall'altro, a semplificarne la struttura. Si è trattato, tuttavia, di tentativi tanto numerosi quanto vani, emarginati (e a volte dimenticati) nei meandri delle aule parlamentari [22], e il cui fallimento lascia presagire come unica alternativa ai vuoti di tutela nel contempo diffusisi, altri interventi "*spot*" tra loro disorganici e confusi.

9.4. *I margini di applicabilità delle nuove tecnologie nel diritto penale agro-alimentare*

L'impatto delle nuove tecnologie sul settore agroalimentare, se da un lato evidenzia la crisi del tradizionale modello punitivo, dall'altro impone un ripensamento della disciplina in una chiave moderna. L'agognata (e sperata) riforma dell'intera normativa di settore dovrebbe, infatti, volgere la propria attenzione verso soluzioni che meglio si adattano alle dinamiche delle nuove condotte fraudolente, che si avviluppano tanto negli intricati e moderni circuiti commerciali della distribuzione (come, per l'appunto, l'*e-commerce*), caratterizzati dalla mancata coincidenza dell'operatore a cui sia riferita la messa in circolazione degli alimenti con quello a cui sia imputabile la minaccia di aggressione, quanto nella speri-

[22] Il primo – e forse più immaturo – dei progetti di legge risale al 2009, con cui si prevedeva una riforma radicale del Titolo VI del libro II del codice penale con l'obiettivo di un aggiornamento rispetto sia al modello di tutela della sicurezza alimentare profilatosi in Europa a partire dal Regolamento 2002/178/CE. Per un approfondimento analitico relativo all'articolato, si veda, *ex pluris*, M. DONINI, *Il progetto di riforma dei reati in materia di sicurezza alimentare*, in *Cass. pen*., 12, 2010, p. 4457 ss.; ID., *Reati di pericolo e salute pubblica. Gli illeciti di prevenzione alimentare al crocevia della riforma penale*, in *Riv. trim. dir. pen. econ.*, 1-2, 2013, p. 45 ss. Più coerente con l'obiettivo qui indicato di riduzione e semplificazione del sistema punitivo è invece il più recente progetto della Commissione Caselli del 2015, che, ragionando su un modello penalistico di disciplina, si concentrava (soprattutto, ma non solo) sul contenuto decisamente poco chiaro dell'art. 5 d.lgs. n. 238/1962, selezionando le condotte più rilevanti della filiera alimentare attraverso una progressività della tutela valutata in termini di offensività e colpevolezza. Questa impostazione avrebbe consentito una sensibile opera di depenalizzazione e, nel contempo, una riorganizzazione scalare della tutela, modulata sulla compresenza di illeciti amministrativi e fatti penalmente rilevanti, prevedendosi ipotesi sia delittuose sia contravvenzionali, con tipologie sanzionatorie variabili in relazione all'ambito della grande distribuzione o del commercio all'ingrosso. Per un approfondimento sullo schema di disegno di legge con le relative linee guida si veda C. CUPELLI, *Il cammino verso la riforma dei reati in materia agroalimentare*, in *www.dirittopenalecontemporaneo.it*, 2 novembre 2015; altresì, S. CORBETTA, *Brevi note a margine del progetto di riforma dei delitti alimentari contro la salute pubblica*, in *Dir. pen. proc*., 11, 2015, p. 1343 ss.; ancora M. DONINI, *Il progetto 2015 della Commissione Caselli*, cit., p. 12.

mentazione genetica dei prodotti alimentari, in cui è più facile che *tante sostanze non allarmanti si sommano in maniera allarmante* [23].

In questo mutato contesto di riferimento, l'impiego delle nuove tecnologie potrebbe fornire sicuramente un notevole contributo per sviluppare e ottimizzare metodi analitici e scientifici in grado di assicurare, da un lato, l'autenticità dei prodotti agroalimentari, con un miglioramento delle loro qualità, e, dall'altro, una rapidità nell'accertamento delle violazioni. Ed è proprio in questa prospettiva, cioè in termini di prevenzione più che di repressione, che deve ragionarsi quando si pensa all'applicabilità nel diritto agroalimentare di nuovi e moderni strumenti tecnologici.

La previsione di un nuovo sistema di tracciabilità digitale del prodotto lungo la filiera agroalimentare rappresenta, ad esempio, uno primo strumento promettente di *law enforcement* in grado di rafforzare l'attuale modello preventivo delle frodi alimentari e migliorare la sicurezza alimentare: una più nitida segmentazione delle fasi, infatti, facilita l'identificazione, e conseguente responsabilizzazione, dell'operatore eventualmente coinvolto nella violazione delle norme relative alla propria parte del processo produttivo. Adeguata a tale scopo è l'uso della tecnologia cd. *blockchain*, un registro pubblico al cui interno sono registrate migliaia di transazioni crittografate, ognuna delle quali è collegata ad un soggetto specifico (i cosiddetti "blocchi") che, collegate tra loro attraverso un sistema di marche temporali, creano un vero e proprio *database* a catena (*chain*) in continuo aggiornamento e liberamente consultabile dagli utenti. Tali blocchi sono convalidati da soggetti *ad hoc*, i cd. *miners*, che utilizzano *software* ed *hardware* specializzati: una volta validati, sui nuovi blocchi viene apposta una marca temporale che permette di aggiornare la *blockchain* mantenendo un certo ordine cronologico all'interno della stessa. Ogni nuovo blocco verrà così inserito all'interno del registro condiviso, riprodotto nei vari dispositivi accrescendo dunque la sicurezza dei dati contenuti nei vari blocchi; ciò permette a tutti gli utenti di avere un controllo sui dati in esso contenuti. In tal modo, i dati contenuti nei vari blocchi risultano immutabili, e comunque immuni da modifiche [24].

[23] Così U. BECK, *Risikogesellschaft. Auf dem Weg in eine andere Moderne*, Frankfurt am Main, 1986, trad. it. *La società del rischio*. *Verso una seconda modernità*, Carocci, Roma, 2000, p. 35. La sperimentazione genetica degli alimenti, infatti, se da un lato offre un apparente miglioramento delle qualità del prodotto, dall'altro porta con sé nuovi rischi da ignoto cd. (bio-)tecnologico circa la loro eventuale pericolosità o innocuità per la salute del consumatore, dapprima imprevisti. Per un approfondimento sui rischi dell'ignoto biotecnologico, si rinvia a L. STORTONI, *Angoscia tecnologica ed esorcismo penale*, in AA.VV., *Il rischio penale da ignoto tecnologico*, Giuffrè, Milano, 2002, p. 85 ss.

[24] Per un approfondimento delle applicazioni della *blockchain* nel settore agro-alimentare, si veda in particolare G. SPOTO, *Gli utilizzi della "Blockchain" e dell'Internet of Things*

Nel caso di prodotti agricoli, ad esempio, il sistema potrà archiviare i dati sul terreno di coltivazione, le sementi impiegate, i tempi di semina e raccolto, i trattamenti fitosanitari, o, nel caso di prodotti di origine animale (si pensi alla mozzarella di bufala), i dati riguardanti gli stabilimenti di origine, le modalità di lavorazione, i trattamenti medici, le condizioni di allevamento [25]. Si consente così al consumatore di conoscere l'intero percorso del prodotto e degli elementi che compongono un determinato alimento.

Considerando che un prodotto alimentare su dieci risulta adulterato, contraffatto o comunque etichettato in modo errato, grazie a questa tecnologia i prodotti manomessi possono essere facilmente identificati e isolati, con un enorme vantaggio in termini di velocità d'intervento e di tutela della *food safety* [26].

Peraltro, il consolidamento di un simile gestionale – pur considerando le luci e le ombre ad essa associate [27] – può rivelarsi una leva strategica per l'affermazione di altre tecnologie che si servono di questo strumento per il loro corretto funzionamento: dall'applicazione di un'etichetta interattiva provvista di *QR code*, con cui si offre al consumatore, in maniera diretta, semplice e intuitiva, l'accesso a tutte le informazioni del prodotto, al cd. *fingerprinting*, ovvero "l'impronta digitale" metabolomica degli alimenti che, grazie all'elevato dettaglio informativo, si presta allo sviluppo di sistemi automatizzati capaci in pochi secondi di riconoscere le caratteristiche salienti di un prodotto, così da identificarlo in ogni passaggio della filiera, dalla produzione sino al consumo [28].

nel settore degli alimenti, in *Riv. dir. alim*., 1, 2019, p. 25 ss. Più recentemente, sempre G. SPOTO, *Il mercato agroalimentare nell'era digitale innanzi all'emergenza Covid-19,* in *Riv. dit. alim*., 1, 2021, p. 54 ss.

[25] Ad esempio, qualora un caseificio concorrente provi ad alterare l'etichetta dei propri prodotti asserendo di aver usato il lotto di latte precedentemente tracciato con la *blockchain*, la frode risulterà facilmente individuabile dalle autorità in quanto i codici impiegati dalla filiera del prodotto autentico risulteranno già utilizzati e quindi non reimpiegabili.

[26] Nel contrasto alle frodi, e in particolare alle sofisticazioni alimentari, l'ENEA, Agenzia nazionale per le nuove tecnologie, l'energia e lo sviluppo economico sostenibile, ha recentemente sviluppato un nuovo strumento tecnologico, cd. *Safefood*, ovvero un laser fotoacustico che permetterà a industrie alimentari e grandi catene di distribuzione di rintracciare elementi contaminanti prelevando una piccola quantità di prodotto. La tecnologia alla base di questa importante innovazione è la spettroscopia, già attiva in campo medico, con un funzionamento basato su luce e suono. La luce del laser è modulata a una frequenza acustica che a contatto con il campione di cibo genera un'onda captata da un microfono.

[27] Tra i particolari vantaggi della *blockchain* vi è la particolare versatilità di questa tecnologia, che consente di realizzare obiettivi di decentralizzazione, tracciabilità, trasparenza, sicurezza e immutabilità dei dati. Tra le ombre, emerge quelle relative ai termini di gestione e implementazione del sistema, che se "sovraccaricato" potrebbe implodere, con il rischio di rallentare il sistema di validazione.

[28] Per un maggiore approfondimento si rinvia all'interessante articolo di V. GALLO (a cu-

L'effettiva capacità preventiva di un sistema di tracciabilità del prodotto così ragionato richiede, tuttavia, che da un lato tutti gli operatori coinvolti nel processo produttivo e distributivo siano dotati di tecnologie compatibili, in modo da tracciare integralmente l'*iter* dalla materia prima alle nostre tavole, e, dall'altro, che il legislatore riconosca identità giuridica a questo nuovo strumento di certificazione, presidiandone la modalità di sviluppo e di applicazione.

Infatti, nonostante i vantaggi, specie nella valorizzazione delle eccellenze enogastronomiche italiane, la tecnologia basata sulla *blockchain* fatica ancora ad affermarsi, non solo per lo spirito tendenzialmente conservativo delle imprese agroalimentari, ma anche, e soprattutto, perché il suo funzionamento, coinvolgendo tutti gli operatori della filiera, comporta importanti investimenti finanziari che, senza aiuti economici statali, difficilmente possono essere sostenuti. Per colmare questo *gap*, in data 6 dicembre 2021 il Ministro Giancarlo Giorgetti ha firmato il decreto attuativo del Fondo per lo sviluppo delle tecnologie e delle applicazioni di intelligenza artificiale, *blockchain* e *internet of things*, istituito presso il Mise, con una dotazione iniziale di 45 milioni di euro, che ha l'obiettivo di promuovere la competitività e la produttività del sistema imprenditoriale del Paese attraverso progetti di ricerca e innovazione tecnologica legati al programma transizione 4.0.

Sul piano della normazione, tuttavia, l'adozione di sistemi di *blockchain* all'interno della filiera agro-alimentare è però un tema ancora poco scrutinato, con la sovrapposizione di ambiti disciplinari al contempo privatistici e pubblicistici che rendono la sua applicabilità molto complessa [29]. In questa direzione si accoglie con favore il timido passo intrapreso dal cd. "Decreto Semplificazione e innovazione digitale" (d.l. 16 luglio 2020, n. 76, convertito con l. 11 settembre 2020, n. 120), con cui si è sancito esplicitamente che «l'utilizzo di tecnologie basate su registri distribuiti produce gli effetti giuridici della validazione temporale elettronica di cui all'art. 41 del Regolamento 2014/910/UE» [30]. Questo tra-

ra di), *Agroalimentare e intelligenza artificiale: la nuova frontiera nelle certificazioni e nella lotta alle frodi alimentari*, in *www.tekneco.it*, 23 marzo 2021. I casi di *fingerprinting* sono sempre più diffusi. Si pensi al caso di alcuni bovini per lo più di *razza limousine* a cui saranno applicati dei chips all'arrivo nelle stalle. Da qui in poi tutte le fasi, incluse la macellazione, la lavorazione, il *packaging* e il trasporto a temperatura fino ai canali di distribuzione, saranno tracciate con l'assegnazione del *food passport*, certificato tramite *blockchain* che raccoglie e conserva in un ID digitale unico tutte le caratteristiche verificate e certificate del prodotto, consultabili dal consumatore in modo semplice e intuitivo tramite la scansione di un *QR Code* che sarà apposto sull'etichetta della confezione.

[29] Per una valutazione dei limiti della *blockchain*, cfr. N. DI PAOLA, *Blockchain e supply chain management*, Cedam, Padova, 2018, p. 80 ss.

[30] Il cd. "Decreto Semplificazione e innovazione digitale" (d.l. 16 luglio 2020, n. 76, convertito con l. 11 settembre 2020, n. 120), con il quale, definite preventivamente le tecnologie

guardo, peraltro, contribuisce a realizzare gli obiettivi di introduzione di un unico sistema integrato dei controlli, individuato dal Regolamento 2017/625/UE, che – come è noto – è stato approvato soprattutto per semplificare e razionalizzare i controlli dinanzi all'eccessiva pluralità delle fonti dopo l'introduzione del Pacchetto igiene e le successive integrazioni [31]. Si consentirebbe così di attuare, in modo sistemico, un'effettiva integrazione degli strumenti di controllo ufficiali del settore agro-alimentare, non soltanto a fini igienico sanitari, ma anche in tema di qualità dei prodotti.

Le lacune nella disciplina tuttavia sono ancora tante e restano soprattutto con riguardo all'esigenza di garantire l'affidabilità dei controlli e dei dati affidati ai computer in rete: anche perché il sistema permette di validare le informazioni sia sotto il profilo temporale, sia sotto il piano dell'immutabilità, ma non garantisce la correttezza e la veridicità delle informazioni. Anzi: più aperta (e quindi potenzialmente più grande) è la catena, maggiore sarà la difficoltà di individuazione del gestore unitario sovraordinato cui attribuire la responsabilità per eventuali prodotti alimentari che risultino in qualche modo contraffatti [32].

basate su registri distribuiti quali «le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile, simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili», sancisce esplicitamente che «l'utilizzo di tecnologie basate su registri distribuiti produce gli effetti giuridici della validazione temporale elettronica di cui all'art. 41 del Regolamento 910/2014/UE».

[31] Per un approfondimento sulla abbondante opera di regolamentazione europea, si rinvia ancora a L. CARRARA, *Dal Regolamento (UE) 2017/625 alle misure applicative unionali e nazionali: un percorso innovativo ma non concluso*, in *Riv. dir. alim*., 4, 2020, pp. 37-47; ancora, F. ALBISINNI, *Il Regolamento (UE) 2017/625: controlli ufficiali, ciclo della vita, impresa e globalizzazione*, in *Riv. dir. alim.*, 1, 2018, pp. 11-36.

[32] Cfr. G. TEUBNER, *Soggetti giuridici digitali?*, Giuffrè, Napoli, 2019, pp. 26-37, il quale utilizza l'espressione «lacune di responsabilità» per evidenziare che la dinamica della digitalizzazione produce spazi vuoti che le categorie giuridiche attuali non sono in grado di interpretare e comprendere in modo adeguato: «fino a quando la dogmatica persisterà nel reagire alle nuove realtà digitali con lo strumentario concettuale tradizionale, continueranno ad emergere carenze nella disciplina della responsabilità». In particolare sono tre i rischi in materia di responsabilità derivanti dalla digitalizzazione: 1) il rischio di autonomia, nelle ipotesi di decisione prese direttamente dalla macchina; 2) il rischio di associazione, derivante dalla cooperazione tra uomo e agente *software*; 3) il rischio di interconnessione, che riguarda l'ipotesi di una pluralità di computer in rete.

9.5. *Ridurre per adeguare; semplificare per rinnovare*

Perché le nuove tecnologie possano assolvere efficacemente una loro funzione preventiva, è necessario che l'intero sistema punitivo venga ripensato alla radice. La natura «*palesemente ribelle*» [33] della materia, infatti, produce (troppe) lacune che i classici strumenti di diritto penale non riescono ad arginare con tempestività: dal "rischio da sviluppo" [34] delle metodologie innovative alle responsabilità del certificatore, nel caso della *blockchain*, o, più in generale, degli operatori che le utilizzano. L'assenza di una normativa adeguata alla diffusività dei nuovi strumenti tecnologici, peraltro, rischia di essere colmata nel breve periodo da interventi arbitrari della giurisprudenza o da una scomposta normazione di *soft law*, che anziché garantirne l'efficienza applicativa, potrebbe favorirne il loro illecito uso. Emerge così un vero e proprio "diritto dell'incertezza", che attribuisce agli operatori del settore – dal produttore al giudice – responsabilità non adeguatamente presidiate.

Per garantire i numerosi vantaggi offerti dalle nuove tecnologie in tema di produzione quanto di circolazione dei prodotti alimentari, più sicuri sia a tutela dei consumatori sia dei produttori, è allora improcrastinabile procedere con una riforma dell'attuale quadro normativo della materia. Nondimeno, occorre essere cauti nell'individuazione delle nuove coordinate da seguire.

L'inefficienza della disciplina vigente esclude anzitutto l'opportunità di perseverare con lo strumento intrinsecamente penale. Da un lato, infatti, la rigidità strutturale del tipo astratto di illecito si è rivelata incompatibile sia con la flessibilità della casistica criminologica, sia con riguardo alla nuova dimensione tecnologica del fenomeno; dall'altro, l'accentuazione di un modello di prevenzione dell'illecito, che ricorre peraltro all'uso sregolato di eccessive tecniche di tutela a forma anticipata attraverso l'applicazione indiscriminata di moderni strumenti di rilevazione, sembra elidere la natura di *extrema ratio* del diritto penale.

La costruzione di un efficiente sistema di prevenzione e repressione degli illeciti alimentari può, invece, meglio esprimersi attraverso un recupero della centralità delle sanzioni amministrative, le quali, per propria natura, si mostrano strutturalmente più adeguate a promuovere la tutela della sicurezza alimentare "*dalle e con*" le nuove tecnologie [35], meglio adattandosi alla nuova prospettiva

[33] È definita così già nel 1971 da G. AZZALI, *Osservazioni in tema di frodi alimentari*, in AA.VV., *Problemi penali in tema di frodi alimentari*, Giuffrè, Milano, 1971, p. 135.

[34] Si pensi all'ipotesi, ad esempio, in cui il danno alla salute sia provocato dal consumo di nuovo alimento autorizzato in base alle conoscenze tecniche del momento e successivamente, invece, non confermate.

[35] Cfr. G. TOSCANO, *Suggestioni del Lebensmittelstrafrecth in vista di una riforma degli illeciti agroalimentari*, in *Riv. it. dir. proc. pen*., 4, 2020, p. 1843 ss.

"autorizzativa-procedimentale" della disciplina. La centralità delle nuove metodologie, in particolare quelle di (ri)tracciabilità del prodotto, infatti, comporterà inevitabilmente un irrobustimento dei procedimenti amministrativi di autorizzazione, quanto degli obblighi formali da adempiersi per la distribuzione e circolazione degli alimenti. Questo nuovo modello di tutela, che potrebbe definirsi "a liceità condizionata", richiede tuttavia come condizione indispensabile una preliminare razionalizzazione, "per sottrazione", della pletora di illeciti amministrativi oggi presenti: solo così, infatti, si attribuirebbe una concreta effettività al sistema, migliorando l'efficacia dissuasiva delle previsioni.

Nondimeno, la radice penale non può essere estratta completamente in ragione della permanenza di taluni fatti che per gravità e diffusività richiedono controlli più penetranti e maggiori garanzie in sede di accertamento [36]. Anche in questo caso, tuttavia, l'efficienza del sistema dipende da un'accurata selezione degli illeciti da qualificare come penalmente rilevanti. Solo così si potrebbe migliorare l'efficacia general-preventiva delle fattispecie rimanenti – vecchie o nuove –, attribuendo loro un più elevato grado di tassatività, determinatezza e, dunque, di applicabilità. Simile opzione, peraltro, darebbe nuovamente lustro e centralità alle ipotesi contravvenzionali previste, in particolare, dagli artt. 5, 6 e 12 della legislazione speciale (l. n. 283/1962). D'altronde, nonostante il fallito tentativo di una abrogazione *tour court* [37], il sistema contravvenzionale risulta ancora essenziale

[36] Cfr. S. CORBETTA, *Sicurezza alimentare da "ignoto biotecnologico"*, cit., pp. 2257-301.

[37] Il «colpo di spugna» di un'abrogazione "quasi" integrale della disciplina igienico sanitaria della produzione e della vendita delle sostanze alimentari e delle bevande prevista dalla l. n. 283/1962 si è avuto per effetto dell'art. 18, comma 1, lett. b) e c) del d.lgs. 2 febbraio 2021, n. 27, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2017/625 ai sensi dell'articolo 12, lettere a), b), c), d) e e) della l. 4 ottobre 2019, n. 117". Nondimeno, le unanime preoccupazioni per gli effetti della *abolitio criminis* – dalla retroattività delle abrogazioni relative alle contravvenzioni agroalimentari al vuoto di tutela per i consumatori in ragione della natura puramente amministrativa delle violazioni – sono tuttavia venute meno con il d.l. n. 42/2021 ("Misure urgenti sulla disciplina sanzionatoria in materia di sicurezza alimentare"), con cui il Consiglio dei Ministri, modificando la disciplina introdotta con il decreto n. 27/2021, ha escluso, prima della sua entrata in vigore, gli effetti abrogativi in relazione agli illeciti alimentari di cui agli artt. 5, 6, 12 e 12 *bis* della l. n. 283/1962. In tal modo, intervenendo prima della scadenza del termine ordinario di *vacatio legis*, si è mantenuta la loro rilevanza penale, scongiurando, nel contempo, le conseguenze iper-retroattive delle abrogazioni normative concernenti le contravvenzioni alimentari. Per un approfondimento, si veda A. NATALINI, *Colpo di spugna sui reati alimentari: abrogate le contravvenzioni igienico-sanitarie minori*, in *Norme e tributi plus, il Sole 24 ore*, 13 marzo 2021, p. 2; G. AMENDOLA, *Leggi alimenti: si rimedia a un errore*, in *Quest. giust.*, 31 marzo 2021; F. DIAMANTI, *Il sortilegio di Von Kirchmann. Abrogati (nottetempo) i reati alimentari della l. n. 283/1962*, in *Sistema penale*, 17 marzo 2021, p. 1 ss.; E. MAZZANTI, *Abrogata la legge 30 aprile 1962, n. 283: una scelta incomprensibile che rischia di aprire una voragi-*

per garantire la sicurezza e l'igiene degli alimenti e, probabilmente, lo strumento più adeguato per accogliere un diritto penale "leggero" «dal punto di vista probatorio e sanzionatorio». La sua efficace operatività dipende, tuttavia, da una riforma che, oltre ad aggiornamento contenutistico delle previsioni contravvenzionali, riesca anche ad attenuare la tensione con le previsioni codicistiche. In effetti, sembra questa la direzione intrapresa quantomeno dagli ultimi progetti di legge maturati in seno all'aula parlamentare [38], sebbene poi falliti per ragioni principalmente politiche [39].

Alla sottrazione – in termini sia di quantità sia di qualità – dei caotici precetti penali, dovrebbe tuttavia affiancarsi anche una semplificazione dei complessi, e spesso inarrivabili, snodi disciplinari della normazione. In questa direzione, l'opzione di affidarsi a un testo unico – peraltro già immaginata con il progetto di riforma del 2009 [40] – dovrebbe considerarsi ancora percorribile [41], se finalizzata a offrire agli operatori della filiera, e del diritto, una mappatura più omogenea e ordinata della disciplina [42]. Il che implica, però, non una mera trasposizione in

ne nel sistema degli illeciti alimentari, in *Giur. pen. web*, 3, 2021, p. 1 ss.; G. AMENDOLA, *L'assurda abrogazione della "legge alimenti". Sguarnito il fronte della tutela della salute dei cittadini e del contrasto delle frodi alimentari*, in *Quest. giust*., 19 marzo 2021, p. 1 ss.

[38] Per un richiamo ai recenti progetti di riforma della disciplina, si veda la nota 21.

[39] Secondo parte della dottrina, infatti, i fallimenti devono attribuirsi «a ragioni di scelte politico – criminali che non si vogliono intraprendere, essendo questo settore troppo nevralgico, quasi un crocevia, rispetto ad alcuni temi centrali della riforma del codice e dei suoi rapporti con le leggi complementari, oltre alla circostanza politico – parlamentare che sono numerosi, i Ministeri cointeressati a tali riforme: Giustizia, Salute, Ambiente, Sviluppo economico, Politiche Agricole». Così M. DONINI, *Reati di pericolo e salute pubblica. Gli illeciti di prevenzione alimentare al crocevia della riforma penale*, in *Riv. trim. dir. pen. econ.,* 2013, p. 87.

[40] Si trattava di un proposito perseguito dalla legge delega 7 luglio 2009, n. 88, all'art. 7, modulato sullo schema del Codice del Consumatore poco prima emanato con il d.lgs. n. 206/2005. Un progetto percorribile, ma che comunque, come ragionato, non avrebbe risolto alcuni problemi di fondo ineludibili: costruire precetti culturalmente pregnanti, chiari, e orientativi rispetto al senso ultimo delle condotte. Per un approfondimento sul progetto, si rinvia a A. GARGANI, *Reati contro l'incolumità pubblica*, cit., p. 267 ss.

[41] In tal senso, potrebbe essere utile un confronto con il sistema tedesco che, pur condividendo con la nostra disciplina una *climax* ascendente di gravità sanzionatoria delle condotte, le cui ipotesi più gravi si rinvengono nello *Strafgesetzbuch*, si avvale di un testo normativo unitario, il *Lebensmittel- und Futtermittelgesetzbuch* (LFGB), che accorpa la disciplina penale e amministrativa di settore. Per un approfondimento sul raffronto comparatistico con il sistema tedesco di repressione degli illeciti alimentari, si rinvia ancora a G. TOSCANO, *Suggestioni del Lebensmittelstrafrecth in vista di una riforma degli illeciti agroalimentari*, cit., p. 1845 ss.

[42] Cfr. M. DONINI, *Il progetto 2015 della Commissione Caselli*, cit., p. 10, nota 19, che

un testo unitario di strumenti normativi accumulatisi nel tempo, oramai inadeguati a offrire ragionevolezza di scopo e di sistema, ma un'indispensabile attività selettiva e una strutturazione teleologicamente orientata a riconoscibili obiettivi di tutela, nel rispetto del quadro dei principi fondamentali. Diversamente, l'operazione si risolverebbe – come troppo spesso è accaduto nella nostra legislazione – nella predisposizione di un contenitore vuoto, composto dalla semplice aggregazione delle previsioni previgenti, senza alcun beneficio in termini di prevenzione e contrasto alla criminalità.

9.6. *Conclusioni*

L'applicazione delle nuove tecnologie al settore agroalimentare accentua inevitabilmente le disfunzioni dell'originario impianto sanzionatorio predisposto dal legislatore. Le nuove istanze securitarie, infatti, impongono necessariamente una rivisitazione dei classici strumenti di prevenzione, che devono essere ripensati rispetto alle nuove forme di aggressione della sicurezza alimentare.

Il percorso di ristrutturazione è tuttavia tortuoso e soprattutto lontano. L'*impasse* decennale della riforma, da un lato, e la malsana prassi di colmare i vuoti di tutela con esasperazioni precettistiche, tipica degli ultimi anni, dall'altro, mostra la difficoltà, sicuramente tecnica, di approcciare ad una materia estremamente complessa, e attorno alla quale gravitano enormi interessi economici. Ciò peraltro rallenta un processo di maturazione dell'identità prevalentemente amministrativa della materia, che, se acquisita, consentirebbe di operare una semplificazione della disciplina attraverso una attenta riduzione del coacervo penale. Un modello con una simile fisionomia, infatti, non solo attribuisce pragmatismo alle ipotesi astrattamente previste, in grado peraltro di adattarsi velocemente alle mutevoli condizioni empiriche, ma attraverso l'impiego delle innovazioni tecnologiche consentirebbe anche – e soprattutto – interventi anticipati di tutela basati su nuove logiche di tipo precauzionale. Al contempo, l'attribuzione all'illecito amministrativo della centralità sanzionatoria nella prevenzione dei nuovi rischi consentirebbe alla sanzione penale di (ri-)assumere con rigorosa razionalità ed efficacia il suo ruolo "accessorio", occupando il campo solo in caso di violazioni estremamente peculiari o gravi. In questa direzione sembra, d'altronde, volgere il recente d.d.l. A.C. n. 2427/2020, recante "Nuove norme in materia di illeciti agro-alimentari" che, ripercorrendo soluzioni normative già proposte con precedenti progetti poi naufragati, riserva al diritto penale la sola protezione

muove grandi perplessità sulla concreta capacità di riordino del legislatore, che non avrebbe «una *mens* ordinatrice».

di fatti pericolosi per la sicurezza alimentare, e dunque anche per la salute pubblica [43]. Peccato, però, che sia tutto fermo [44].

[43] Il disegno di legge qui richiamato in verità riprende, in parte, i contenuti del precedente d.d.l. S. n. 2231/2016, con il quale era stato recepito il progetto di riforma del diritto sanzionatorio agroalimentare elaborato dalla Commissione Caselli istituita nel 2015 presso l'ufficio legislativo del Ministero della Giustizia, e poi confluito nel quasi integralmente nel d.d.l.S. n. 283. Per un approfondimento sul testo, si rinvia a D. CASTRONUOVO, *La riforma dei reati a tutela della salute pubblica e della sicurezza alimentare. Appunti sul D.D.L. 2427*, in *Sistema penale*, 14 dicembre 2020.

[44] Dal sito istituzionale della Camera dei Deputati, infatti, il disegno risulta "bloccato" dal 23 aprile 2020 in II Commissione Giustizia *in sede* Referente.

Elenco Curatori e Autori

Giuseppe Alesci, Avvocato e Dottore di ricerca in Diritto penale.

Giuliano Balbi, Professore ordinario di Diritto penale. Università degli Studi della Campania Luigi Vanvitelli.

Fabio Basile, Professore ordinario di Diritto penale. Università degli Studi di Milano La Statale.

Alberto Cappellini, Giudice presso il Tribunale di Spoleto. Dottore di Ricerca in discipline penalistiche. Università degli Studi di Firenze.

Marco Colacurci, Ricercatore di Diritto penale. Università degli Studi della Campania Luigi Vanvitelli.

Federica De Simone, Ricercatrice di Diritto penale. Università degli Studi della Campania Luigi Vanvitelli.

Mariavaleria del Tufo, Professoressa straordinaria di Diritto penale. Università degli Studi Suor Orsola Benincasa.

Andreana Esposito, Professoressa associata di Diritto penale. Università degli Studi della Campania Luigi Vanvitelli.

Stefano Manacorda, Professore ordinario di Diritto penale. Università degli Studi della Campania Luigi Vanvitelli.

Antonio Pagliano, Ricercatore di Diritto processuale penale. Università degli Studi della Campania Luigi Vanvitelli.

Chiara Pistilli, Dottoranda di Diritto penale. Università degli Studi della Campania Luigi Vanvitelli.

Gaspare Jucan Sicignano, Avvocato e Ricercatore di Diritto penale. Università degli Studi Suor Orsola Benincasa.

Finito di stampare nel mese di dicembre 2022
nella Stampatre s.r.l. di Torino – Via Bologna 220