UNO SGUARDO OLTRE LA *COMPLIANCE* 231: *DIGITAL CRIMINAL COMPLIANCE* E RISCHIO DI INFILTRAZIONI MAFIOSE NELLE IMPRESE

di Mattia Di Florio
(*Assegnista di ricerca in diritto penale presso l'Università di Foggia*)

SOMMARIO: 1. Premessa. Il sistema di *compliance* 231 e le imprese: un rapporto "difficile". – 2. (segue) Il rilievo dell'analisi del rischio nel sistema *compliance* 231. 3. (segue) La *mancanza di compliance* 231 *ed il rischio di infiltrazioni criminali nella c.d. Covid economy*. – 4. (segue) Il PNRR ed i riflessi normativi sul sistema di *compliance* 231 in materia di prevenzione di infiltrazioni mafiose: profili di criticità. – 5. *Compliance* 231 e *biases* dei giudici: cenni. – 6. Guardando oltre la *compliance 231*: la *digital compliance*. – 7. (segue) La *digital compliance*: l'*IA* ed il *machine learning* nuovi (possibili) strumenti predittivi delle infiltrazioni mafiose nelle imprese. – 8. (segue) La *digital compliance*, il problema *black box*. – 9. (segue)...ed altri problemi. – 10. Conclusioni.

1. È noto che il Decreto n. 231/2001 sulla responsabilità da reato degli enti[1] ha introdotto nel nostro ordinamento il sistema di *compliance programs* (di seguito, c*ompliance* 231), sulla base dell'esperienza anglosassone[2].

Tale sistema può essere inteso, in generale, come un insieme di regole e procedure volte a prevenire, attraverso una preventiva valutazione del rischio le violazioni delle norme che potrebbero dar luogo alla responsabilità della società[3].

Alla *compliance* 231 si sono ormai adeguate le medie e grandi imprese, ad eccezione di quelle micro e piccole[4].

[1] Sulla natura della responsabilità degli enti (*ex* D.lgs. n. 231/2001), che è stata oggetto di un annoso dibattito dottrinale tra sostenitori delle teorie penale, amministrativa e di *tertium genus*, e che sembra essersi ricomposto più di recente a favore di quest'ultima opzione ermeneutica, v. *funditus* O. Di Giovine, *Lineamenti sostanziali del nuovo illecito punitivo*, in G. Lattanzi (a cura di), *Reati e responsabilità degli enti*[2], Milano 2010, 3 ss.; nonché, anche a favore di tale ultima tesi, A. Manna, *La responsabilità dell'ente da reato tra sistema penale e sistema amministrativo: riflessioni rapsodiche su offensività, colpevolezza e sistema sanzionatorio*, in D. Piva (a cura di), *La responsabilità degli enti ex d.lgs. n. 231/2001 tra diritto e pro*cesso, Torino 2021, 3 ss. e, spec., 12 ss.

[2] Per l'analisi dei *compliance programs* americani, v. *amplius*, O. Di Giovine, *Lineamenti sostanziali del nuovo illecito punitivo*, cit.; più di recente, C.E. Paliero, *Il sistema sanzionatorio dell'illecito dell'ente: sistematica e rationale*, in *RIDPP*, 4, 2021, 1199 ss.

[3] V. *funditus* G. Presti, *What We Talk About When We Talk About Compliance*, in S. Manacorda – F. Centonze (a cura di), *Corporate Compliance on a Global Scale. Legitimacy and Effectiveness*, Springer 2022, 25 ss.

[4] V. *Prevenzione e governo del rischio di reato: la disciplina 231/2001 e le politiche di contrasto dell'illegalità nell'attività di impresa*, in *www.assonime.it*, 14 marzo 2019. Le imprese medie hanno un numero tra i 50 e i 249

Ci si potrebbe chiedere quali siano le ragioni di una così non uniforme implementazione della *compliance* 231, tanto più se si considera che le micro imprese costituiscono i due terzi della comunità imprenditoriale nazionale[5], e le piccole aziende contribuiscono (con le medie imprese) al 41% dell'intero fatturato generato in Italia, al 33% di tutti gli occupati del settore privato ed al 38% del valore aggiunto del Paese»[6].

Una delle possibili spiegazioni è che l'adozione della *compliance* non è obbligatoria[7], poiché il Decreto 231 prevede, al massimo, un onere della prova a carico dell'ente di aver adottato ed efficacemente attuato un MOG per essere esente da responsabilità per i reati commessi nel suo interesse o a suo vantaggio da soggetti apicali (art. 6, D.Lgs. 231), o da soggetti sottoposti per inosservanza degli obblighi di direzione e vigilanza (art. 7, D.lgs. 231)[8].

Inoltre, è ancora diffusa la convinzione, rimasta anche durante la pandemia Covid-19[9], che il sistema di *compliance* 231 sarebbe incompatibile per aziende molto piccole dove le funzioni sono concentrate nelle mani di poche persone, e dove la *compliance* è percepita come un "peso" burocratico e, quindi, un "costo" aziendale, piuttosto che uno strumento di sicura utilità per i processi organizzativi e gestionali[10].

Un'ulteriore ragione sembra evocare il dilemma del prigioniero della teoria dei giochi[11]. Attraverso il Decreto 231, lo Stato mira a prevenire e reprimere i reati

addetti ed un fatturato non superiore a 50 milioni di euro; le grandi imprese 249 dipendenti ed un fatturato superiore a 50 milioni di euro. Le microimprese hanno meno di 10 occupati ed un fatturato non superiore a 2 milioni di euro; le piccole imprese 50 dipendenti ed un fatturato non superiore a 10 milioni di euro.

[5] V. i dati ISTAT relativi al primo censimento delle imprese, svolto tra maggio e ottobre 2019, e diffuso già all'inizio di febbraio 2020, sono reperibili in *www.istat.it*

[6] Secondo i dati dell'Osservatorio del Politecnico di Milano, v. *Innovazione Digitale nelle PMI*, in *www.osservatori.net*. Inoltre, la metà delle PMI è concentrata nel Nord secondo i dati ISTAT citati *supra*.

[7] Un punto di contatto tra i compliance programs americani e quelli del Decreto 231 è la non obbligatorietà della loro adozione da parte degli enti, v. *funditus* Di Giovine, *Lineamenti sostanziali del nuovo illecito punitivo*, cit., 87 ss.

[8] In argomento v. *amplius* N. Mazzacuva- E. Amati, *Diritto penale dell'economia*[5], Milano 2020, 57 ss.

[9] V. *Gli effetti del Covid-19 sulle PMI. Il modello 231 da status symbol a dispositivo di protezione*, in *www.altalex.com*, 28 maggio 2020.

[10] I dati ISTAT relativi al primo censimento delle imprese, svolto tra maggio e ottobre 2019, e diffuso già all'inizio di febbraio 2020, sono reperibili in *www.istat.it*

[11] In argomento, v. *funditus*, F. Centonze, *Responsabilità da reato degli enti e agency problems*, in *RIDPP*, 2017, 3, 945 ss.

Il dilemma del prigioniero è un problema di teoria dei giochi (in argomento v. O. Morgestern, *Teoria dei giochi, uno strumento per lo studio di fatti economici e sociali*, trad. it., Milano 1969).

Anche se il nome del dilemma fa riferimento ad un prigioniero si può formulare come un gioco tra due delinquenti. Due prigionieri tenuti in celle distinte, e senza la possibilità di cooperare tra loro, devono scegliere se collaborare o non collaborare con l'Autorità, sapendo che se uno collabora accusando l'altro, chi ha collaborato evita la pena; l'altro viene però condannato a 7 anni di carcere; se entrambi accusano l'altro, vengono entrambi condannati a 6 anni; se nessuno dei due collabora, entrambi vengono condannati a 1 anno. Contrariamente a quanto previsto dagli assiomi di razionalità di Pareto che imporrebbero a ciascun prigioniero di non collaborare, accade, invece, che ognuno dei delinquenti segue la strategia di confessare per massimizzare la propria utilità, indipendentemente dalla scelta dell'altro (c.d. equilibrio di Nash). Infatti, la strategia di collaborare esporrebbe ciascun prigioniero al rischio di una pena da 0 a 6 anni, mentre la strategia

societari; le imprese hanno interesse a minimizzare il rischio di responsabilità penale adottando la *compliance* 231; in teoria, dovrebbe esserci collaborazione tra Stato e imprese, ma ciò non avviene nella pratica a causa della "reciproca diffidenza alla collaborazione". Questo perché l'organizzazione privata è tenuta a investire grandi risorse nella *compliance*, ma ogni beneficio della cooperazione è rimandato all'accertamento giudiziario attraverso il quale si ricostruisce *ex post* la regola di condotta che si sarebbe dovuta adottare; il soggetto collettivo, invece, non fidandosi dell'offerta di benefici da parte dello Stato e temendo imprevedibili conseguenze sanzionatorie, è portato a limitare l'onere della prevenzione e ad adottare metodi di *compliance* formali e di facciata; allo stesso modo, nei casi in cui si verifichi un reato, l'impresa, in assenza di un accordo affidabile e di una sicura "ricompensa" per la collaborazione, non favorisce l'emersione dell'illecito, sperando di neutralizzare il rischio di un aumento della responsabilità[12].

Tanto premesso sul "difficile" rapporto tra la *compliance* 231 e (parte delle) aziende, cercheremo di chiarire nei prossimi paragrafi l'importanza del sistema di *compliance* non solo a livello generale, ma soprattutto come strumento per prevenire ed evitare il rischio di infiltrazioni mafiose.

2. Nell'ambito della *compliance* 231 i modelli organizzativi di gestione (MOG 231, d'ora in poi) individuano i settori di attività in cui possono essere commessi i reati e redigono la relativa mappatura del rischio-reato (i cc.dd. *Control Self Assessment* e *Risk Management*)[13].

La valutazione del rischio (il c.d. *risk assessment*) riveste una notevole importanza ai fini della redazione del MOG 231, anche se la sua portata è potenzialmente "indeterminata", in quanto il legislatore non ha individuato gli elementi caratterizzanti la condotta preventiva dell'ente[14].

---

di non collaborare al un rischio di pena da 1 a 7 anni (in argomento v. AA.VV., *Dilemma del prigioniero e strategie dominanti*, Milano 2011).

[12] F. Centonze, *Responsabilità da reato degli enti e agency problems*, cit., 946.

[13] Sulle caratteristiche dei modelli organizzativi di gestione del rischio, si rinvia a O. Di Giovine, *Lineamenti sostanziali del nuovo illecito punitivo*, cit., 96 ss.

[14] V. in argomento, S. Manacorda, *L'idoneità preventiva dei modelli di organizzazione nella responsabilità da reato degli enti: analisi critica e linee evolutive*, in *RTDPE*, 2017, 59 ss.; A. Manna, *Controversie interpretative e prospettive di riforma circa la responsabilità da reato degli enti*, in *Riv. trim. dir. pen. econ.*, 2015, 155 ss.; più di recente sul punto, A. De Lia, *La responsabilità da reato dell'ente*, in A. Manna – A. De Lia (a cura di), *Dieci nodi gordiani di diritto penale dell'economia*, Milano 2021, 21, cui si rinvia per gli opportuni riferimenti bibliografici, dove si evidenzia che «il legislatore non ha definito in modo puntuale gli elementi e le caratteristiche che debbono connotare l'azione preventiva dell'ente collettivo, rimettendone la definizione alla prudenza di quest'ultimo, che rappresenta un'obbligazione "di mezzi" (l'adozione della migliore strategia possibile, la c.d. *best practice*) e non "di risultato" (in termini di impedimento dell'illecito); si tratta evidentemente di una sfaccettatura sistematica di estrema criticità, poiché la valutazione della correttezza della condotta tenuta dall'ente – in difetto di parametri certi – finisce col formare oggetto di una valutazione giudiziaria che si rivela giocoforza, dal contenuto fortemente discrezionale, e che determina un alto tasso di imprevedibilità del giudizio».

A tal proposito, appaiono significative le aggiornate Linee Guida sul Modello 231, emanate da Confindustria [15], che ripercorrono gli approcci ermeneutici sul "perimetro" dello sforzo preventivo dell'impresa in termini di valutazione dei rischi.

Secondo la suddetta associazione di categoria, è necessario definire il concetto di "rischio accettabile", ovvero la soglia entro la quale le azioni dell'ente sono fattibili ed esigibili. Questa osservazione deriva dal fatto che «il Decreto 231 impone degli standard normativi che il MOG deve necessariamente rispettare per essere considerato idoneo a prevenire i reati»[16].

Nei reati dolosi, la "soglia di accettabilità" del rischio si basa sul requisito della "elusione fraudolenta" del sistema di prevenzione (*ex* art. 6 del D.Lgs. 231); a tal proposito, le Linee Guida richiamano la giurisprudenza di legittimità che ha chiarito come, ai fini del Decreto 231, il concetto di condotta fraudolenta consista in una elusione delle misure di sicurezza in grado di disattendere l'efficacia preventiva[17].

Per i reati colposi, invece, laddove non vi sia l'intenzione di realizzare l'evento dannoso (come, ad es., i reati in materia di salute e sicurezza sul lavoro e quelli ambientali), la soglia di accettabilità viene ricondotta al concetto di colpa di organizzazione (*Organisationsverschuld*)[18], ossia il verificarsi di una condotta «in violazione del modello organizzativo e di prevenzione, nonostante la puntuale osservanza degli obblighi di vigilanza previsti dal Decreto 231»[19].

L'intento delle Linee Guida di Confindustria è chiaramente quello di coniugare la finalità di prevenzione del sistema di *compliance* 231 con una precisa analisi di valutazione del rischio, tale da rendere ragionevole l'azione preventiva dell'ente. Allo stesso tempo, si suggerisce alle aziende di basare la valutazione del rischio su di un approccio di *compliance* "integrato" che includa i Sistemi di Gestione qualificati (es. ISO 45001 o ISO 14001), al fine di garantire un flusso costante e coerente di informazioni all'Organismo di Vigilanza (OdV) e di migliorare l'efficienza nella prevenzione dei reati[20].

3. A questo punto, ci si potrebbe chiedere se le aziende prive del sistema di *compliance* 231 siano più esposte al rischio di infiltrazioni criminali.

[15] V. F. Sardella, *Le nuove Linee Guida 231. Principi consolidati e rilevanti novità nell'edizione 2021*, in *www.ilpenalista.it*, 9 settembre 2021.
[16] F. Sardella, *Le nuove Linee Guida 231*, cit.,
[17] V. in giurisprudenza Cass. 30.01.2014, n.4677, in *Dejure*; in dottrina, v. G. Salcuni, *La valutazione di idoneità dei modelli ed il requisito dell'elusione fraudolenta*, in *RTDPE*, 2015, 873 ss.
[18] Sul concetto di *Organisationsverschuld* v. *funditus* K. Tiedemann, *La responsabilità penale delle persone giuridiche nel diritto comparato*, in *Riv. it. dir. proc. pen.*, 1995, 615 ss.
[19] F. Sardella, *Le nuove Linee Guida 231*, cit.
[20] F. Sardella, *Le nuove Linee Guida 231*, cit.

Come è noto, il "nodo" mafia-impresa è un fattore che influenza l'economia legale in molti modi (es. controllo, condizionamento o infiltrazione delle aziende), ampiamente documentato dalla ricerca sociologica [21].

Il "contagio mafioso" è un fenomeno che colpisce le imprese su tutto il territorio nazionale. La metafora epidemiologica del "contagio" (come quella militare dell'"avanzata") rischia, però, di essere fuorviante. La ricerca sociologica sulle infiltrazioni mafiose al Nord evidenzia l'esistenza di un processo di "ibridazione" tra interessi mafiosi e imprenditoriali (la c.d. area grigia), dove la cultura economica «sembra facilitare il dialogo tra imprenditori e criminalità»[22].

Il rischio di infiltrazione sembra aggravarsi nelle fasi di emergenza dell'economia, come dimostrano i quattro *Report* elaborati dall'Organismo permanente di monitoraggio e analisi sul rischio di infiltrazione mafiosa nell'economia segnata dalla pandemia di Covid-19 (la c.d. *Covid economy*) [23].

Il 1° *Report* evidenzia il pericolo che le consorterie criminali approfittino del bisogno di liquidità delle imprese per insinuarsi nella struttura aziendale e portare il denaro necessario o proporre prestiti usurari, fino a configurare uno scenario di *doping* finanziario, articolato su più livelli, dalla concessione di prestiti usurari a piccole imprese operanti in ambito locale alla partecipazione a operazioni di acquisizione di pacchetti azionari di *global player* attivi sui mercati internazionali [24].

Tra i settori imprenditoriali più esposti all'usura mafiosa, nonché al rischio di impossessamento delle attività economiche per il riciclaggio e il rimpatrio dei capitali, vi sono molti settori (quali la filiera agroalimentare, l'edilizia e le costruzioni, la sanità, la ristorazione e i servizi connessi alla persona, la salute, il turismo, l'abbigliamento, il commercio all'ingrosso, la vendita e il noleggio di auto, i servizi funerari e cimiteriali)[25].

Inoltre, nella c.d. *Covid economy*, le associazioni mafiose sembrano impiegare lo strumento delle variazioni societarie per inquinare il tessuto economico produttivo (come il *turnover* delle cariche, il *turnover* delle partecipazioni, il trasferimento delle

[21] In argomento v. *funditus* C. Visconti, *Proposte per recidere il nodo mafie imprese*, in *www.penalecontemporaneo.it*, 7 gennaio 2014. Nella letteratura sociologica, v. *amplius* A. Sciarrone (a cura di), *Alleanze nell'ombra. Mafie ed economie locali in Sicilia e nel Mezzogiorno*, Roma 2011; più di recente, v. A. Sciarrone – L. Storti, *Le mafie nell'economia legale. Scambi, collusioni, azioni di contrasto*, Bologna 2019.

[22] A. Scaglione, *Circuiti criminali e area grigia. Una ricerca sulla presenza delle mafie nel Nordest*, in *Quaderni di Sociologia*, 79, 2019, 165 ss.

[23] Ci si riferisce, in particolare ai quattro *Report* del 23 aprile 2020, del 15 giugno 2020, del 15 settembre e di dicembre 2020, reperibili in *www.interno.gov.it*

[24] V. 1° *Report* del 23 aprile 2020, cit.

[25] V. 1° *Report* del 23 aprile 2020, cit.
Una mafia "al passo con in tempi", non meno pericolosa di altre organizzazioni criminali, è la "Società foggiana" capace di infiltrarsi in modo capillare nel tessuto socio-economico (più di recente, v. in argomento A. Laronga, *Quarta mafia. La criminalità organizzata foggiana nel racconto di un magistrato sul fronte*, Roma 2021).

quote, il trasferimento delle società, quello delle sedi, le variazioni della natura giuridica e/o del capitale sociale)[26].

Il 5° *Report* evidenzia una variazione percentuale del + 7% delle segnalazioni per operazioni sospette nel 2020 rispetto al 2019 e un aumento del + 9,7% del numero di imprese colpite da provvedimenti interdittivi antimafia nel periodo marzo 2020 - febbraio 2021 rispetto allo stesso periodo dell'anno precedente. A tal fine, la Relazione citata individua specifiche fattispecie criminose sintomatiche di condotte che riflettono il pericolo di infiltrazione mafiosa, in quanto reati di maggiore allarme sociale, attorno ai quali gravita con più ampia regolarità statistica il mondo della criminalità organizzata di tipo mafioso, e che costituiscono la base dell'istruttoria per l'emissione di provvedimenti interdittivi da parte del Prefetto[27]: il riferimento è alle estorsioni, al riciclaggio, al trasferimento fraudolento e al possesso ingiustificato di valori, alla turbativa d'asta e così via (i cc.dd. reati spia)[28].

In conclusione, i suddetti dati, registrati durante la c.d. *Covid economy*, sembrano suggerire una risposta affermativa alla domanda iniziale: la mancata adozione del sistema di *compliance* 231 contribuisce ad esporre le imprese, soprattutto quelle più deboli e meno "strutturate", ad un maggior rischio di infiltrazione mafiosa; esse "in cambio" di contiguità criminali, anche solo occasionali, possono beneficiare di liquidità o, comunque, di una riduzione dei costi aziendali.

4. Nel contesto *post*-pandemico, caratterizzato dall'aumento dei prezzi delle materie prime, dell'energia e dei generi alimentari, è prevedibile il rischio di infiltrazioni criminali nei fondi del Piano Nazionale di Ripresa e Resilienza (PNRR) per l'accesso al *Next Generation EU* (noto anche come *Recovery Fund*)[29].

Il legislatore è intervenuto con il D.L. n. 152/2021 recante disposizioni urgenti per l'attuazione del PNRR[30], che prescrive, in un'ottica di "prevenzione collaborativa",

[26] V. 1° *Report* del 23 aprile 2020, cit.

[27] Sui "reati spia" dei provvedimenti interdittivi prefettizi, v., in giurisprudenza, Cons. Stato, 27.11.2018 n. 6707, in *Dejure*.

[28] Il citato 5° *Report* prende, inoltre, in considerazione i reati tributari previsti dal decreto legislativo 10 marzo 2000, n. 74, che comprende diverse fattispecie penali (quali la dichiarazione fraudolenta, dichiarazione infedele, omessa dichiarazione, emissione di fatture per operazioni inesistenti, omesso versamento IVA e omesso versamento di ritenute, distruzione di documenti contabili, indebita compensazione e sottrazione fraudolenta al pagamento di imposte) che, sebbene non tipizzati dal legislatore nelle condotte rientranti nei c.d. "reati spia", rappresentano indicatori altrettanto significativi. Sempre più indagini e dichiarazioni di collaboratori di giustizia hanno, infatti, evidenziato come la criminalità organizzata utilizzi largamente il sistema delle false fatturazioni e delle cosiddette "frodi carosello" per ripulire il denaro ed ottenere vantaggi fiscali.

[29] V. la Relazione semestrale gennaio – giugno 2021 del Ministro dell'Interno al Parlamento sull'attività svolta e risultati conseguiti dalla Direzione Investigativa Antimafia (DIA), in *www.direzione investigativaantimafia.interno.gov*

[30] Il D.L. n. 152/2021 è stato pubblicato in G.U. n. 265/2021 e successivamente convertito in l. 29 dicembre 2021, n. 233.

l'obbligo di attuazione del MOG 231 da parte delle imprese che hanno subito tentativi di infiltrazione mafiosa; a tal fine è stata riformulata la procedura per l'applicazione delle interdittive prefettizie contenute nel c.d. codice antimafia (D.lgs. n. 159/2011).

Il nuovo art. 94-*bis* del Codice antimafia consente al Prefetto, che accerti, nell'ambito della prevenzione amministrativa, tentativi di infiltrazione mafiosa riconducibili a situazioni di occasionale agevolazione, di prescrivere all'impresa, l'adozione e l'efficace attuazione del MOG 231, al fine di rimuovere e prevenire le cause di occasionale agevolazione.

A ben considerare, la summenzionata disposizione sembra però travisare il significato del sistema di *compliance* 231 che ha principalmente una funzione preventiva rispetto ai reati (*compliance* preventiva) e una funzione reattiva quando viene commesso uno dei reati-presupposto (*compliance* reattiva)[31].

Un ulteriore possibile "travisamento" delle funzioni della *compliance* 231 sembra rinvenirsi nel controllo giudiziario delle imprese (art. 34-*bis* del cod. antimafia), che assume la "duplice veste" di provvedimento autonomo dall'amministrazione giudiziaria (art. 34 cod. antimafia), o sua naturale prosecuzione quando vengono meno le condizioni che la legittimavano, ma che ancora non consentono di considerare il contesto aziendale completamente libero da infiltrazioni mafiose[32].

Con il provvedimento che dispone il controllo giudiziario, il tribunale può imporre all'impresa l'obbligo di adottare ed effettivamente attuare il MOG 231 (art. 34-*bis*, co. 2, lett. b, e co. 3, lett. d, cod. antimafia); il programma di risanamento aziendale finisce, dunque, per "rimodellare" le funzioni preventive di *compliance* 231 a favore di una "bonifica postuma" (in linea con un certo orientamento della giurisprudenza di merito)[33].

In breve: il mancato coordinamento con le misure di prevenzione antimafia sembra aver condotto alla previsione di un "anomalo" sistema di *compliance* 231, nell'ambito di una presunta "prevenzione partecipata" tra Stato ed aziende contro le infiltrazioni mafiose[34].

---

[31] Sulle funzioni del MOG nel sistema di *compliance* 231, V. Mongillo, *Presente e futuro della compliance penale. Riflessioni a margine di S. Manacorda e F. Centonze (a cura di), Corporate compliance on a Global Scale. Legitimacy and Effectiveness, 2022*, in *www.sistemapenale.it*, 11 gennaio 2022.

[32] V. in argomento L. Del Favero – C. Corsaro, *L'estensione delle misure di prevenzione patrimoniale ai reati comuni. Amministrazione giudiziaria e controllo giudiziario quali occasioni per la predisposizione degli strumenti di organizzazione, gestione e controllo aziendale*, in *GP*, 2021, 1-*bis*.

[33] In questo senso, v. L. Del Favero – C. Corsaro, *L'estensione delle misure di prevenzione patrimoniale*, cit. Per riferimenti alla giurisprudenza di merito prima e dopo l'entrata in vigore del cod. antimafia, v. *funditus* C. Visconti, *Contro le mafie non solo confisca ma anche "bonifiche" giudiziarie per imprese infiltrate: l'esempio milanese*, in *www.penalecontemporaneo.it*, 20 gennaio 2012; v. anche ID., *Proposte per recidere il nodo mafie-imprese*, in *www.penalecontemporaneo.it*, 7 gennaio 2014; ID., *Ancora una decisione innovativa del Tribunale di Milano sulla prevenzione antimafia nelle attività imprenditoriali*, in *www.penalecontemporaneo.it*, 11 luglio 2016; più in generale, sul tema, v. anche A. Manna, *Misure di prevenzione e diritto penale: una relazione difficile*, Pisa 2019, 83 ss.

[34] In senso contrario si veda L. Del Favero – C. Corsaro, *L'estensione delle misure*, cit.

5. Supponiamo che la *compliance* 231 venga adottato e attuato dall'ente e, tuttavia, il rischio di infiltrazione mafiosa si verifichi. Ci si potrebbe chiedere quale sia l'esito del giudizio di prognosi postuma sull'idoneità *ex ante* del modello di comportamento a prevedere e prevenire il reato del tipo di quello che si è verificato.

È ipotizzabile che l'esito del giudizio sia negativo, a causa di distorsioni cognitive (*biases*), sintomatiche della forte "commistione" tra la sfera emotiva e il ragionamento giudiziario, che portano frequentemente la giurisprudenza «ad elevare l'asticella della pretesa comportamentale ad un livello irrealistico», soprattutto se si considera «la continua espansione dei reati-presupposto a molteplici ambiti della criminalità d'impresa (dalla corruzione ai reati societari, alla frode in commercio, ai *market abuse*, ai reati informatici, ai reati fiscali, ai reati ambientali e alla salute e sicurezza sul lavoro)»[35].

Sono concetti che risalgono alla fine degli anni '70, quando il famoso psicologo Kahneman e il suo collega Tversky iniziarono una lunga collaborazione per studiare la documentazione dei *bias* e le "euristiche" del pensiero intuitivo nelle decisioni razionali. Nel risolvere un problema, la mente tende a seguire strategie cognitive che non corrispondono al ragionamento logico-deduttivo (euristiche), e che sono manifestazioni di *bias* [36].

Gli studi di psicologia del processo penale hanno chiarito la possibile importanza di alcuni *biases* nel processo decisionale dell'organo giudicante, che portano erroneamente a trarre relazioni causali non logicamente corrette (*post hoc propter hoc*), a sovrastimare la probabilità (*insight bias*), o a formulare un giudizio di prevedibilità sotto l'influenza della natura favorevole o infausta dell'evento (*outcome bias*).

Un'ulteriore trappola cognitiva che si verifica frequentemente nel giudizio prognostico è la fallacia della probabilità "*a priori*" (c.d. fallacia dell'accusatore), che sostanzialmente sovrastima la probabilità di accadimento dell'evento che la regola precauzionale *ex ante* avrebbe dovuto neutralizzare [37].

Gli effetti dei *biases* nella valutazione retrospettiva dell'idoneità della *compliance* 231 avrebbero un duplice effetto negativo per le imprese. In primo luogo, il probabile esito negativo del giudizio di prognosi postuma potrebbe indurre le aziende a seguire rigidamente il principio di precauzione nell'attuazione della *compliance*, al punto da esporre teoricamente l'impresa al rischio di paralisi; in secondo luogo, non è da

[35] D. Perrone, *La prognosi postuma tra distorsioni cognitive e software predittivi*, Torino 2021, 62-63.
[36] V. *funditus* D. Kahneman, *Pensieri lenti e veloci*, trad. it., Milano 2018, spec. 145 ss.
[37] D. Perrone, *La prognosi postuma tra distorsioni cognitive e software predittivi*, 56 ss.

escludere neppure quello di un disincentivo all'attuazione del sistema di *compliance*[38].

6. La rivoluzione digitale (la c.d. quarta rivoluzione industriale)[39] è destinata a innovare anche il sistema di *compliance* aziendale (come ad es. già avvenuto nel settore finanziario)[40].

Componenti essenziali della *compliance* digitale sono l'intelligenza artificiale (IA) ed il *machine learning* (l'apprendimento automatico).

L'IA è una disciplina recente dell'informatica che cerca di permettere ai *computer* di "fare i tipi di cose che le menti possono fare"[41]; i sistemi di IA elaborano processi computazionali, basati su sequenze di istruzioni algoritmiche di *machine learning* utilizzate, ad esempio, per l'elaborazione di mega-dati (i cc.dd. *Big Data*) da *supercomputer* in grado di eseguire miliardi di calcoli al secondo[42].

Il *machine learning* fa parte, secondo alcuni, dell'informatica e/o della statistica e non dell'IA, ma, secondo altri, non ci sono confini netti in questi campi[43]; qualunque sia la "cornice" degli algoritmi di *machine learning*, non c'è dubbio che essi siano diventati gli "oracoli" dell'era digitale[44].

Le brevi considerazioni di cui sopra permettono di intuire l'importanza che l'IA ed il *machine learning* potrebbero avere, in generale, per l'organizzazione e la gestione

[38] D. Perrone, *La prognosi postuma tra distorsioni cognitive e software predittivi*, cit., 63.

[39] Su IA e quarta rivoluzione industriale v. più di recente, S. Manzocchi, L. Romano, *Io, robot? L'intelligenza artificiale ai temi della quarta rivoluzione industiale*, in P. Severino (a cura di), *Politica economia, diritto, tecnologia*, Luiss University Press 2022, 13 ss.

[40] V. M.C.M. Mozzarelli, *Digital Compliance: The Case for Algorithmic Transparency*, in S. Manacorda – F. Centonze (a cura di), *Corporate Compliance on a Global Scale*, cit., 259 ss.

[41] V. in argomento *funditus* M. Boden, *L'intelligenza artificiale*, trad. it., Bologna 2019, 7 ss.

[42] M. Boden, *L'intelligenza artificiale*, cit., 47, dove si osserva che «il *machine learning* si basa oggi su complicatissime tecniche matematiche, perché le rappresentazioni della conoscenza utilizzate coinvolgono la teoria della probabilità e la statistica». Sul *machine learning*, v. *amplius* P. Domingos, *L'algoritmo definitivo. La macchina che impara da sola e il futuro del nostro mondo*, trad. it., Torino 2016; più di recente, v. G. F. Italiano, E. Prati, *Storia, tassonomia e sfide future dell'intelligenza artificiale*, in P. Severino (a cura di), *Politica economia, diritto, tecnologia*, cit., 22 ss.
Sul piano etimologico, la parola algoritmo deriva dal nome di un matematico e sapiente arabo Al-Khwarizmi, vissuto nel IX secolo d.C., il quale contribuì in maniera significativa allo sviluppo della teoria delle equazioni algebriche (così C. Toffalori, *Algoritmi*, Bologna 2015, 18-19).

[43] M. Boden, *L'intelligenza artificiale*, cit., 47 ss., dove si osserva che il *machine learning* ha tre ampie tipologie: l'apprendimento supervisionato, l'apprendimento non supervisionato e l'apprendimento per rinforzo. Nell'apprendimento *supervisionato*, «il programmatore "addestra" il sistema definendo un insieme di risultati attesi per una data gamma di input (chiamati esempi e non-esempi) e fornendo continue valutazioni del raggiungimento o meno dei risultati». Nell'apprendimento *non supervisionato*, «l'utilizzatore non fornisce né risultati attesi né messaggi di errore; l'apprendimento è guidato dal principio secondo cui i tratti che cooccorrono generano aspettative sul fatto che cooccorreranno in futuro». Infine, l'apprendimento *per rinforzo* «è guidato da analoghi della ricompensa e della punizione: messaggi di feedback che dicono al sistema cosa è stato fatto bene e cosa è stato fatto male». Più di recente, v. anche G. F. Italiano, E. Prati, *Storia, tassonomia e sfide future dell'intelligenza artificiale*, in P. Severino (a cura di), *Politica economia, diritto, tecnologia*, cit., 24 ss.

[44] V. *amplius* A. Vespignani, *L'algoritmo e l'oracolo*, Milano 2019.

dei processi produttivi aziendali (così come per la creazione di nuovi modelli di *business*).

7. L'innovazione digitale, sotto la "spinta" del suddetto PNRR[45], potrebbe essere un'opportunità per le aziende (almeno per quelle medio-grandi) di dotarsi di un sistema di *compliance* in ambito penale (*digital criminal compliance*, d'ora in poi) [46], in grado di potenziare la capacità predittiva della valutazione del rischio-reato rispetto alla *compliance* 231.

Nel nuovo settore *legal-tech*, che punta ad integrare le nuove tecnologie nelle attività legali[47], esiste già un *software* in grado di garantire i due indicatori primari dell'adeguatezza della *compliance 231*: la sua idoneità a prevenire la commissione dei reati-presupposto, e la sua effettiva attuazione da parte dell'organizzazione. Questi *software* permettono di monitorare costantemente il sistema di controllo e di attuare le modifiche normative in modo rapido e preciso, verificabile in tempo reale[48].

Se, ad esempio, una modifica normativa introducesse un nuovo reato nel "catalogo 231", il *software* aggiornerebbe il sistema di *compliance* con un ricalcolo automatico del rischio in relazione al nuovo reato, in modo che il *management* possa avere piani di trattamento coerenti con la propria organizzazione e propensione al rischio[49]. Allo stesso modo, in caso di cambiamenti organizzativi o di *governance*, il *software* aggiornerebbe automaticamente ogni sezione di *compliance*, effettuando anche una rivalutazione del rischio del sistema di controllo [50].

Un sistema di *digital criminal compliance* potrebbe avvalersi della potenza computazionale di algoritmi di *machine learning* "addestrati" a riconoscere i possibili scenari critici aziendali derivanti dal rischio di infiltrazione mafiosa. Il *machine learning* sarebbe in grado di estrarre dai *data set* le informazioni (il c.d. *data mining*) necessarie a identificare i *pattern* ricorrenti per riconoscere tali rischi; l'IA potrebbe, quindi, calcolare il rischio di infiltrazione e aggiornare automaticamente il sistema di *compliance* 231.

Ciò richiederebbe una condivisione dei *data set* a favore di tutte le aziende interessate, al fine di creare una visione sistemica della *digital criminal compliance*; è ipotizzabile che una crescita nel tempo porti alla condivisione di grandi volumi di

[45] Sul punto v. i dati diffusi dall'Osservatorio del Politecnico di Milano, *Innovazione digitale: nel 2022 gli investimenti in ICT cresceranno del 4%*, in *www.osservatori.net*

[46] In argomento v. *funditus* V. Mongillo, *Presente e futuro della compliance penale*, cit.; v. anche P. Severino, *Le implicazioni dell'intelligenza artificiale nel campo del diritto con particolare riferimento al diritto penale*, in P. Severino (a cura di), *Politica economia, diritto, tecnologia*, cit., 29 ss.

[47] In generale, sulle implicazioni tecnologiche dell'IA per il diritto, v. *funditus* A. Santosuosso, *Intelligenza artificiale e diritto. Perché le tecnologie di IA sono una grande opportunità per il diritto*, Milano 2020.

[48] *Compliance 231, il supporto del software nell'adeguamento dei modelli organizzativi*, in *www.digital4.biz*

[49] *Compliance 231*, cit.

[50] *Compliance 231*, cit.

dati, che potrebbero rendere più efficiente la capacità di previsione algoritmica. Quest'ultima ipotesi sembra, al momento, improbabile, visto che, almeno tra le PMI, non più di un terzo esegue analisi predittive, che nella maggior parte dei casi sono molto semplici e i cui risultati sono difficili da integrare nei processi decisionali[51].

Nonostante le difficoltà che si frappongono a un sistema integrato di *digital criminal compliance*, ci sarebbe più di un beneficio: il *machine learning* potrebbe assistere l'impresa nelle operazioni di *due diligence* [52] in occasione di acquisizioni/cessioni societarie o trasferimenti d'azienda; inoltre l'IA sarebbe in grado, in teoria, di "suggerire" all'impresa, nella scelta dei *partners* commerciali, di non considerare quelle aziende che statisticamente presentano indici sintomatici di contiguità mafiosa, se non, appunto, mafiose esse stesse.

8. Il sistema di *digital criminal compliance* presenterebbe anche aspetti critici.

È innanzitutto necessario evidenziare l'opacità del processo decisionale degli algoritmi di *machine learning*, che operano come una "scatola nera" (c.d. *black box*), poiché il processo di calcolo con cui ricevono un *input* per ricavare un *output* non è facilmente interpretabile dall'esterno[53]. Ciò spiega perché gli algoritmi potrebbero anche apparire "ingiusti", come è stato osservato nel diritto penale[54] con riferimento al noto caso Loomis, trattato dalla giurisprudenza anglosassone[55].

---

[51] I. Di Deo, *Predictive Analytics: come "prevedere il futuro" grazie ai dati*, in *www.blog.osservatori.net*

[52] Sul concetto anglosassone di *due diligence*, v. *amplius* Spedding, *The Due Diligence Handbook*, CIMA, 2009.

[53] A. Vespignani, *L'algoritmo e l'oracolo*, cit., 27. Si veda anche D. Spiegelhalter, *L'arte della statistica*, trad. it., Torino 2020, 71 ss. dove, tra le "carenze degli algoritmi", viene evidenzia la mancanza di trasparenza, legata non necessariamente alla loro complessità, in quanto anche semplici algoritmi basati sulla regressione, i cc.dd. algoritmi del rischio di recidiva, come il COMPAS (su cui si veda *infra* nt. 55) «diventano del tutto imperscrutabili se la loro struttura non è pubblica, magari perché coperta dal segreto commerciale».

[54] Più di recente, sia pure con diversità di sfumature, v. M.C.M. Mozzarelli, *Digital Compliance*, cit., 66; O. Di Giovine, *Dilemmi morali e diritto penale*, Bologna 2022, 20. Per una disamina generale del rapporto tra diritto penale ed algoritmi di *IA* si rinvia a C. Burchard, *L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società*, in *RIDPP*, 2019, 4, 1909 ss.

Nell'ambito dell'Unione Europea, dopo che il 3 dicembre 2018 la Commissione per l'efficienza della giustizia del Consiglio d'Europa (CEPEJ) ha approvato la Carta etica sull'uso dell'IA all'interno dei sistemi giudiziari (cfr. *Intelligenza artificiale nella Giustizia: approvata la Carta etica europea*, in www.altalex.com, 4 dicembre 2018), la Commissione europea ha presentato la sua proposta di regolamento sull'IA (cfr. *Intelligenza artificiale, il nuovo quadro normativo europeo*, in www.altalex.com., 17 agosto 2021); il Parlamento europeo ha successivamente approvato una risoluzione sull'uso dell'IA nel diritto penale, chiedendo trasparenza nelle decisioni algoritmiche, (v. *amplius G.* Barone, *Intelligenza artificiale e processo penale: la linea dura del Parlamento europeo. Considerazioni a margine della risoluzione del Parlamento europeo del 6 ottobre 2021*, in *Cass. pen.*, 3, 2022, 1180 ss.).

Per un'analisi comparata sulla regolazione dell'IA in generale, v. *amplius* A. Malaschini, *Regolare l'intelligenza artificiale. Le risposte di Cina, Stati Uniti, Unione europea, Regno Unito, Russia e Italia,* in P. Severino (a cura di), *Politica economia, diritto, tecnologia*, cit., 33 ss.

[55] Il caso *Loomis c. State of Wisconsin*, viene citato come esempio di una possibile discriminazione di genere: in breve i fatti. Nel 2013 Loomis fu arrestato dagli agenti di polizia per resistenza a pubblico ufficiale e ricettazione, dopo essere stato trovato alla guida di un'auto rubata ed impiegata in un precedente conflitto a fuoco nello Stato americano del Wisconsin. Loomis veniva tratto a giudizio e condannato dalla Corte (*Trial Court*) a cinque anni di reclusione e successivi cinque anni di sorveglianza speciale, dopo che il Giudice aveva

Questo non sarebbe tuttavia un problema insuperabile: secondo il famoso matematico americano Steven Strogatz, «non capiremmo perché l'oracolo ha sempre ragione, ma potremmo verificare i suoi calcoli e le sue predizioni con esperimenti e osservazioni e confermare le sue rivelazioni»[56].

Il problema *black box* sembra inoltre sorgere anche per il cervello umano, seppure in una certa misura[57]. Un esempio di ciò si può rinvenire nella matematica, "padrona" e "serva" delle discipline scientifiche[58], dove i percorsi mentali di ragionamento logico-deduttivo che portano dagli assiomi alla dimostrazione dei teoremi non seguono una logica "lineare". Questi ultimi, infatti, sono solo la "punta dell'*iceberg*", mentre restano invisibili (e incomprensibili) i processi mentali che hanno portato il matematico a modificare o perfezionare le ipotesi iniziali (un analogo processo di ricostruzione razionale "*a posteriori*" del processo decisionale si ritrova, ad es., nelle sentenze). Per citare il filosofo ungherese Michael Polanyi, in un problema c'è sempre una conoscenza "implicita", non trasferibile ad altre persone, perché la conoscenza "tacita" guida il percorso cognitivo di un soggetto dal particolare ad una visione coerente del tutto[59].

Ci sarebbe, però, un aspetto critico "collegato" al citato problema *black box*: anche se l'intelligenza algoritmica fosse un giorno in grado di "spiegarsi" da sola, gli esseri umani non riuscirebbero a seguire il suo ragionamento. Esistono già teoremi che sono stati dimostrati dai computer (ad es. il teorema dei quattro colori[60], la congettura di Keplero sul modo più efficiente di posizionare le sfere nello spazio tridimensionale[61]), le cui dimostrazioni, sebbene siano state convalidate, nessuno ha

---

esaminato anche l'elevato livello di pericolosità sociale nel *risk assessment* di recidiva dell'imputato, così come elaborato dal software COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*). Quest'ultimo è un algoritmo predittivo che, alla luce dei dati inseriti nel sistema (*input*) e di un questionario di numerose domande sottoposte al reo, attribuisce un risultato (*outpout*) in termini di punteggio (*score*) circa il rischio di recidiva del reo. L'algoritmo predittivo di COMPAS opera come una *black box* che, nell'ambito dell'intelligenza artificiale, definisce alcuni sistemi di *machine learning* che da un *input* forniscono un *output*, ma nei quali i calcoli che avvengono durante il processo non sono facilmente interpretabili. (sul caso Loomis v. *amplius* F. Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *DPU*, 2019, 10, spec. 21 ss.).

[56] S. Strogatz, *One Giant step for a Chess-Playing Machine*, in *The New York Times*, 26 dicembre 2018.

[57] Va sottolineato che non c'è alcuna ragione logica per cui gli algoritmi di IA debbano funzionare come l'intelligenza umana: sebbene si abbia l'impressione che il nostro cervello e quello artificiale attuino, a volte e in qualche misura, principi strutturali simili, in realtà, sono molto diversi sia per il livello dei materiali di cui sono fatti, sia per il modo in cui agiscono i loro processi di trasmissione dei segnali (v. *amplius* I. Stewart, *I dadi giocano a Dio?*, trad. it., Torino 2020, 85 ss.).

[58] In argomento, v. E. Boncinelli, U. Bottazzini, *La serva padrona. Fascino e potere della matematica*, Milano 2000.

[59] M. Polanyi, *La conoscenza inespressa*, Roma 2018.

[60] Il teorema dei quattro colori è stato dimostrato nel 1977 da Kenneth Appel e Wolfang Haken con l'aiuto di un computer ed afferma che, sotto precisi vincoli, bastano quattro colori a colorare qualsiasi mappa politica, in modo che due nazioni contigue non abbiano mai lo stesso colore (in argomento, v. P. Manca, *Il giallo del teorema dei quattro colori*, Pisa 2018).

[61] Per spiegare la congettura di Keplero, formulata nel 1611, sul c.d. impacchettamento di sfere nello spazio euclideo tridimensionale, si consideri il problema dei fruttivendoli quando devono impilare delle arance in una

potuto verificare completamente[62]. Recentemente, sembra che tecniche di *machine learning* siano state impiegate per "guidare l'intuizione dei matematici" e "aiutare nella scoperta di teoremi e congetture"[63].

Non resta che immaginare un'IA di "livello umano"[64] che un giorno fornisca dimostrazioni che, come diceva il famoso matematico ungherese Paul Erdos, "provengono dalla Bibbia", cioè che rivelino perché una teoria è corretta, senza costringere «ad accettarla a forza di argomenti brutti e difficili»[65].

9. Sussisterebbero, poi, due ulteriori e distinti problemi.

In primo luogo, gli algoritmi di *machine learning*, come gli umani, non sono immuni da pregiudizi (*biases*), che possono dipendere dal tipo di "addestramento" che hanno ricevuto.

Questo effetto si verificherebbe, ad esempio, nell'ipotesi in cui la *digital criminal compliance* impiegasse algoritmi che non sono stati addestrati dai programmatori con dati di "buona qualità"; ciò potrebbe far sì che gli algoritmi associno ad alcune imprese l'etichetta di "alto rischio" di infiltrazione mafiosa, a causa dell'ubicazione della sede legale in contesti ad alta densità criminale, o semplicemente per la provenienza geografica. Tale *bias* porterebbe erroneamente l'algoritmo a suggerire all'ente di non intraprendere collaborazioni commerciali o di non valutare operazioni societarie con una determinata azienda.

Inoltre, anche se l'addestramento del *machine learning* fosse condotto con *data set* di qualità, non si potrebbe escludere che la decisione algoritmica appaia "ingiusta", a causa della mancanza di una definizione matematica univoca di equità[66].

---

cassetta. Ci si chiede quale sia il modo ottimale di disporre le arance (sfere), se posizionarle in strati identici una sull'altra o se distribuirle a strati in modo che ogni sfera si inserisca nel vuoto formato da quattro sfere sottostanti (come fanno i fruttivendoli con le arance). La congettura di Keplero è che il metodo efficiente sia il secondo, ma ci sono voluti più di quattrocento anni per dimostrarlo, quando nel 1998 Thomas Hales l'ha verificata con l'ausilio di algoritmi (per i dettagli tecnici, v. T. Hales et al., *A formal proof of the Kepler conjecture*, in *Forum Math. Pi* (2017), Vol. 5, 1 ss.

[62] S. Strogatz, *Il potere dell'infinito. L'universo raccontato dal calcolo infinitesimale*, trad. it., Torino 2021, 335-336.

[63] In argomento, v. *amplius* S. De Toffoli, *I nodi dell'intelligenza artificiale*, in www.maddmaths.simai.eu, 2 gennaio 2022.

[64] Sullo sviluppo futuristico di un'IA di livello umano, e sulla conseguente creazione di una "superintelligenza" v. N. Bostrom, *Superintelligenza. Tendenze, pericoli, strategie*, trad. it., Torino, 2018.
Vale la pena sottolineare (cfr. D. Spiegelhalter, *L'arte della statistica*, cit., 71-72) che oggi siamo ben lontani da una IA "di livello umano" (la c.d. IA forte) capace di farsi un'idea dei meccanismi causali sottostanti alle associazioni modellate dagli algoritmi. In altre parole, i modelli algoritmici consentono all'IA di rispondere solo a domande come: "abbiamo osservato X, cosa ci aspettiamo di osservare ora?". Al contrario, l'IA "forte" richiede un modello causale di come funziona realmente il mondo, che consentirebbe di rispondere a domande di livello umano sull'effetto di determinati interventi ("cosa succede se facciamo X?") e a controfattuali ("cosa sarebbe successo se non avessimo fatto X?").

[65] S. Strogatz, *Il potere dell'infinito*, cit., 336.

[66] In argomento, v. A. Vespignani, *L'algoritmo e l'oracolo*, cit., 44.

Consideriamo, per esempio, un sistema di *machine learning* che preveda per due gruppi di aziende (A e B) il rischio di avere infiltrazioni criminali dopo un certo periodo di tempo. Supponiamo che il *machine learning* abbia una "parità predittiva", cioè che la sua capacità previsionale corrisponda esattamente a quella dei dati statistici dai quali si osserva che il gruppo A possegga un rischio maggiore di infiltrazioni criminali (doppio) rispetto al gruppo B. Anche se il *machine learning* avesse una simile capacità, sussisterebbe il problema dei "falsi positivi", derivanti dal confronto tra quelle aziende che, sebbene etichettate ad "alto rischio" di infiltrazione criminale (perché appartenenti al gruppo A), in concreto non hanno corso rischi simili, e tutte le altre aziende. Sarebbe, quindi, improbabile che il *machine learning* soddisfi l'equità nel tasso di "falsi positivi" ed impossibile che soddisfi una terza forma di equità, l'equità nel tasso di "falsi negativi"[67], cioè il confronto risultante tra le aziende che hanno subito un'infiltrazione criminale, pur essendo etichettate "a basso rischio", e tutte le altre imprese.

In secondo luogo, i sistemi di *machine learning* non sono "bravi" a riconoscere quando sbagliano, come lo sono gli umani. Per esempio, se la *digital criminal compliance* commettesse un errore nel processo decisionale di prevenzione del rischio di infiltrazione mafiosa, non lo ammetterebbe. Ci si potrebbe chiedere come spiegare questo paradosso.

Ad una prima lettura, sembrerebbe che la spiegazione di una simile "trappola" per l'IA presenti qualche vaga somiglianza con l'*overconfidence bias* che è un *bias* egocentrico (smascherabile con la formula di Bayes), che mina il ragionamento umano[68].

A ben guardare, però, la risposta al suddetto paradosso andrebbe ricercata nei limiti fondamentali della matematica dimostrati dal famoso logico-matematico Kurt Gödel con i suoi teoremi degli anni ′30, in particolare il teorema di incompletezza dei sistemi matematici formali[69], e da Alan Turing che lo "tradusse" in termini di macchine, invece che di sistemi formali (con i quali lavorava Gödel), realizzando il progetto del "calcolatore universale" (il moderno *computer*)[70].

---

[67] A. Vespignani, *L'algoritmo e l'oracolo*, cit., 61.

[68] Sull'*overconfidence bias* v. in letteratura B. Fishhoff, P. Slovic, S. Lichtenstein, *Knowing with certainty: The appropriateness of extreme confidence*, in *Journal of Experimental Psychology: Human Perception and Performance*, 3(4), 1977, 552-564. In argomento, v. più di recente, con particolare riferimento alla formula di Bayes, M. Menale, *Overconfidence bias, occhio alle proprie convinzioni,* in *www.maddmaths.simai.eu,* 21 aprile 2022.

[69] G. Odifreddi, *Il dio della logica. Vita geniale di Kurt Gödel, matematico della filosofia*, Milano 2018.

[70] A. Turing, *On computable numbers, with an application to the entscheindungsproblem*, in *Proceedings of the London Mathematical Society*, Vol. s2-42, Issue 1, 1937, 230.
Uno dei più suggestivi sviluppi teorici di *computer science* riguarda la possibile esistenza di una branca più generale della fisica che potrebbe portare a progettare una macchina che generalizza il *computer* universale. Questa macchina (concettualizzata per la prima volta, in un ambiente di "automi cellulari", dal famoso matematico ungherese Von Neumann), sarebbe capace di operare come un "costruttore universale", vale a dire

Nel già citato teorema di incompletezza del 1931, Gödel dimostrò che in un sistema matematico "usuale", dove c'è la possibilità di usare i numeri naturali (e, quindi, un mondo che oggi definiamo "digitale"), ci sono verità indimostrabili che sono relative a un certo sistema; con un continuo processo di "cambio di sistema" è possibile dimostrare verità che prima erano nascoste, fermo restando che ci saranno altre verità indimostrabili, e così via all'infinito[71].

Allo stesso modo, ci sono alcuni problemi computazionali, come Turing dimostrò più tardi, che non possono essere affrontati da algoritmi, a tal punto da mettere in discussione quella che è stata effettivamente chiamata la "dittatura" del calcolo algoritmico[72].

Qualche decennio dopo, il noto matematico americano Steve Smale propose una lista di 18 problemi matematici irrisolti per il XXI secolo, tra i quali l'ultimo problema riguardava i limiti dell'intelligenza sia per gli esseri umani che per le macchine; un simile problema si riferisce al già citato paradosso mostrato da Gödel e Turing, che continua a ispirare importanti ricerche sui limiti "intrinseci" dei sistemi di IA[73].

Tra le ricerche più recenti, è degno di nota un interessante studio sul problema delle reti neurali artificiali del *deep learning* (l'apprendimento profondo, un "segmento" del *machine learning*)[74], che non sono in grado di capire quando stanno

---

in grado di realizzare tutte le trasformazioni consentite dalle leggi della fisica, non solo calcoli, ma anche costruzioni generali, comprese quelle termodinamicamente permesse (ad esempio, il raffreddamento di vari sistemi), quelle biologiche (ad esempio, l'autoriproduzione e le funzioni biologiche correlate), e molto altro. Si potrebbe concepire questa macchina «come una generalizzazione estrema di una stampante 3D: una volta inserito un programma appropriato e fornita sufficiente materia prima di partenza, il costruttore universale costruirebbe, a partire da essi, qualsiasi sistema permesso dalle leggi della fisica» (in argomento, v. *funditus*, C. Marletto, *La scienza dell'impossibile. Alla ricerca delle nuove leggi della fisica*, trad. it., Milano spec. 232, 2022).

[71] G. Odifreddi, *Il dio della logica*, cit.,70.

[72] P. Zellini, *La dittatura del calcolo*, Milano 2018.
Vi sono classi di problemi per i quali non esistono algoritmi efficienti, il più importante dei quali è il problema del commesso viaggiatore (*Travelling Salesman Problem*, *TSP*) che richiede, dato un insieme di città e distanze note tra ogni coppia di esse, di trovare la distanza minima che un commesso viaggiatore deve percorrere per visitare tutte le città una ed una sola volta e tornare alla città di partenza. Il problema *TSP* può essere associato a un grafo, cioè all'astrazione matematica formata da un insieme di punti (nodi) e un insieme di linee (archi), dove V è l'insieme degli n nodi (o città) e A è l'insieme degli archi (o strade). È stato dimostrato che il *TSP* è un problema NP-difficile (NP-completo per la classe di complessità FP^{NP}), il che significa che non esistono algoritmi efficienti per risolvere il problema *TSP*, poiché la complessità dell'operazione la rende impraticabile per grafi di dimensioni comuni nei problemi reali (v. *funditus* W. J. Cook, *In pursuit of the Traveling Salesman. Mathematics at the Limits of Computation*, Princeton University Press 2012). Più di recente, sulla complessità computazionale, con riferimenti anche alla classe di problemi NP, v. *Computer Scientists Prove That Certain Problems Are Truly Hard*, in *www.quantamagazine.org*, 11 maggio 2022.

[73] Sul punto v. M. Pisani, *Gli errori dell'IA? Li spiegano Turing e Gödel*, in www.maddmaths.simai.eu, 15 aprile 2022.

[74] In argomento, v. M. Boden, *L'intelligenza artificiale*, cit., 79 ss., dove si osserva che le reti neurali artificiali (*ANN*, *Artificial Neural Networks*) sono «composte da molte unità interconnesse, ognuna in grado di computare una e una sola cosa»; esse sono utili per «modellare certi aspetti del cervello, e per il riconoscimento di *pattern* e l'apprendimento»; recentemente queste reti "multistrato" hanno suscitato un certo entusiasmo con l'avvento degli algoritmi di *deep learning*, in cui «il sistema apprende la struttura raggiungendo in profondità un dominio, e non solo pattern superficiali; in altri termini, scopre una rappresentazione della

commettendo errori (il c.d. problema dell'instabilità dell'IA) [75]. I ricercatori sostengono che, in virtù del paradosso dimostrato da Gödel e Turing, non è possibile trovare una soluzione al problema e che solo in casi specifici gli algoritmi di *machine learning* possono portare a reti neurali stabili e accurate; propongono, inoltre, una teoria classificatoria per descrivere quando le reti neurali possono essere addestrate a fornire un sistema affidabile di IA, in certe specifiche condizioni[76].

Dalle precedenti considerazioni si comprende che solo in particolari condizioni gli algoritmi della *digital criminal compliance* potrebbero essere addestrati ad ammettere gli errori commessi; nella generalità dei casi essi mostrerebbero un "eccesso di sicurezza" nella loro capacità di prevedere il rischio di infiltrazione mafiosa nelle aziende, ma solo in casi particolari "riconoscerebbero" i loro limiti previsionali.
La componente umana, quindi, rimane centrale per "sfidare" le previsioni algoritmiche[77].

10. Supponiamo che si verifichi un reato-presupposto che il modello comportamentale di *digital criminal compliance* avesse lo scopo di prevenire. Ci si potrebbe chiedere quale sarebbe l'esito del giudizio prognostico.

Volendo, in conclusione, azzardare una risposta, sussisterebbe però un paradosso: come potrebbe il giudice valutare retrospettivamente eventuali "fallimenti" della regola cautelare algoritmica senza esporsi a potenziali *bias*? Supponiamo che il giudice si avvalga di sistemi artificiali predittivi[78]: anche in tal caso, l'esito della prognosi postuma potrebbe portare ad una decisione non necessariamente esente da errori rispetto a quanto realmente accaduto.

Tale paradosso non sembra, tuttavia, insormontabile se si considera il fatto che il significato di verità processuale non è "assoluto" ma "relativo": se ci fosse una verità (assoluta), il giudice dovrebbe "scoprirla", non "stabilirla" attraverso un verdetto sulla base di prove o testimonianze. In altre parole, il giudice cerca di mettere insieme una "narrazione" che sia coerente con i fatti, ma non c'è modo di provare che questa

---

conoscenza a più livelli, anziché a livello unico».

[75] M.J. Colbrook, A. Vegard, A.C. Hansen, *The difficulty of computing stable and accurate neural networks: On the barriers of deep learning and Smale's 18 th problem*, in PNAS, 16 marzo 2022.

[76] M. Pisani, *Gli errori dell'IA? Li spiegano Turing e Gödel*, cit., 52.

[77] Per un approccio critico al processo decisionale algoritmico v. H. Fry, *Hello World. Esseri umani nell'era delle macchine*, trad. it., Milano 2019.
Con particolare riferimento al diritto penale, evidenzia più di recente il rilievo della decisione umana nei processi di creazione ed interazione con i sistemi artificiali, B. Panattoni, *Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'autonomia artificiale*, in *Dir. Inf.*, 2021, 2, spec. 366-367.

[78] D. Perrone, *La prognosi postuma tra distorsioni cognitive e software predittivi*, cit., 55.
Sulla giustizia digitale, v. *amplius* A. Garapon, J. Lassègue, *La giustizia digitale. Determinismo tecnologico e libertà*, trad. it., Bologna 2021.

"narrazione" sia adeguata e corretta, cioè che sia effettivamente quello che è accaduto nella realtà. Questo è un limite analogo ai teoremi di Gödel[79].

[79] G. Odifreddi, *Il dio della logica. Vita geniale di Kurt Gödel*, cit.