LUISS

Dipartimento di Giurisprudenza

Cattedra di Diritto e Procedura penale degli enti

CRIMINAL COMPLIANCE E NUOVE TECNOLOGIE

Chia.mo Prof. Antonio Gullo

RELATORE

Chia.ma Prof.ssa Francesca Minerva

CORRELATORE

Anna Francesca Romani - 157313

CANDIDATO

ANNO ACCADEMICO 2022/2023

CAPITOLO III

RISCHI E ZONE D'OMBRA DELLA *DIGITAL CRIMINAL COMPLIANCE*

INTRODUZIONE

Nell'ultimo decennio siamo stati testimoni di una vera e propria rivoluzione tecnologica, un processo trasformativo della realtà ad opera dei nuovi paradigmi digitali i quali, in virtù della portata trasformativa che li caratterizza, sono stati capaci di influenzare lo svolgimento di molteplici attività quotidiane prima di sola competenza dell'uomo.

Anche le organizzazioni complesse hanno beneficiato dell'utilizzo di tali nuovi sistemi tecnologici. Queste ultime hanno iniziato ad avvalersi degli algoritmi di intelligenza artificiale nella conduzione di molteplici operazioni interne quali il perfezionamento dei sistemi produttivi, la gestione delle risorse umane e l'organizzazione della *supply chain*, in quanto le stesse garantiscono, in taluni casi, maggiore velocità, efficacia ed efficienza rispetto ad uno svolgimento internamente demandato alle intelligenze umane.

Alla luce dei benefici già apportati nella realizzazione di molteplici operazioni, il presente lavoro si interroga sulla possibilità che le nuove tecnologie, in modo particolare quelle basate sull'Intelligenza artificiale, possano spiegare i propri effetti positivi in un altro settore di particolare interesse per le imprese, vale a dire quello della *compliance* penale.

La *criminal compliance*, infatti, interessa una fetta importante degli investimenti delle società in quanto rappresenta il fulcro di ogni strategia di contrasto alla criminalità che trova terreno fertile nelle organizzazioni complesse. Lo testimonia il ruolo di assoluta centralità che la stessa riveste nel sistema normativo delineato dal d.lgs. 231/2001 sia *ex ante*, in merito ai criteri di imputazione del reato all'ente, che *ex post*, in relazione alle attività riparative che l'ente ha la possibilità di porre in essere dopo la verificazione del reato. Ne consegue un forte incentivo per le *corporations* a predisporre l'insieme di presidi volti a prevenire la commissione di una fattispecie criminosa al suo interno o, qualora il reato si sia già verificato, a realizzare le condotte riparative previste dal decreto con l'obiettivo di ottenere i correlati benefici contemplati dallo stesso.

Ai numerosi risultati positivi conseguibili attraverso l'adozione di un modello organizzativo idoneo, non corrispondono altrettante indicazioni legislative

volte ad indicare in che modo strutturare gli stessi. Il decreto 231 del 2001 si limita, infatti, a fornire un'essenziale ossatura del MOG incapace, da sola, di guidare pienamente le imprese nell'esercizio delle attività tipiche di *compliance*.

Contribuisce ad incrementare il sentimento di incertezza in capo alle persone giuridiche la quasi totale assenza di pronunce giudiziali volte ad attestare l'idoneità di un modello giuridico e il conseguente esonero dell'impresa da ogni profilo di responsabilità.

Per le ragioni sopra illustrate, il presente lavoro intende verificare se ed in che modo perfezionare la costruzione di un modello organizzativo attraverso l'utilizzo dei nuovi paradigmi tecnologici a supporto delle attività tipiche di *compliance* indicate nel decreto 231 del 2001, così da fornire agli enti nuove opportunità per adeguarsi alle normative in vigore e ridimensionare il rischio di verificazione di una fattispecie di reato in azienda.

Il primo capitolo verrà dedicato ad una ricognizione generale funzionale all'indagine delle principali tecnologie sviluppate fino al giorno d'oggi. L'analisi esordirà tracciando alcuni riferimenti storici in merito all'ideazione e allo sviluppo dell'intelligenza artificiale per poi procedere illustrando le principali definizioni di IA, le caratteristiche maggiormente identificative, i procedimenti funzionali alla loro formattazione nonché le modalità di funzionamento delle stesse, tutte basate sullo sfruttamento a vario titolo dei *Big data*.

Un approfondimento specifico verrà poi riservato alle due principali declinazioni d'intelligenza artificiale, vale a dire la *Big data Analysis* e il *Machine Learning*, ponendo l'attenzione sulle differenze che intercorrono tra le stesse in termini di caratteristiche, programmazione e funzionamento in concreto.

Alla panoramica delle principali tecnologie sviluppate seguirà una ricognizione della seppur scarna regolamentazione vigente in materia e dei principali disegni di legge, focalizzando l'attenzione sui cinque principi contemplati dalla Carta Etica Europea e dedicando un'analisi specifica alla proposta di regolamento europeo sull'intelligenza artificiale elaborata dalla Commissione europea e sottoposta all'approvazione del Consiglio e del Parlamento europeo.

L'ultima parte del primo capitolo sarà dedicata ad un approfondimento in merito alle tecnologie a registro distribuito, concentrando l'attenzione sulla

Blockchain e sugli *Smart Contracts* i quali, alla luce dei connotati ontologici che presentano, sembrerebbero prestarsi a molteplici impieghi funzionali alla *compliance* dell'ente.

Segue il secondo capitolo, il quale si concentrerà prima sulle opportunità teoriche derivanti dall'impiego degli strumenti digitali più all'avanguardia, per poi verificare come gli stessi possano rappresentare un valido supporto nelle diverse fasi di costruzione di un modello organizzativo esplicitamente contemplate dal comma 2 dell'articolo 6 d.lgs. 231/2001.

Si fa riferimento alle operazioni di mappatura del rischio, di procedimentalizzazione delle attività e delle decisioni interne, di controllo dei flussi informativi e di monitoraggio dei flussi finanziari, tutti adempimenti indispensabili per un modello che ambisca ad un giudizio positivo di idoneità da parte della magistratura, giudizio propedeutico all'esonero del *tertium genus* di responsabilità ascrivibile all'ente o, comunque, funzionale ad una riduzione delle sanzioni irrogabili nei confronti della persona giuridica.

Infine, l'ultima parte del secondo capitolo sarà dedicata alle *Internal Investigations*, vale a dire all'insieme delle operazioni conoscitive poste in essere dall'ente sia per attestare l'adeguatezza e l'idoneità dei presidi organizzativi adottati, che per fornire all'impresa gli strumenti necessari alla gestione del versante patologico dell'attività collettiva, focalizzando l'attenzione sulla prima finalità perseguita, quella c.d. interna o manutentiva.

Se i primi due capitoli saranno incentrati sui connotati positivi propri dei nuovi strumenti digitali e sulle opportunità di avvalersi degli stessi nella conduzione delle operazioni tipiche di conformità, sarà al terzo capitolo che verrà demandata l'analisi dei rischi e delle zone d'ombre scaturenti dal fenomeno della *Digital Criminal Compliance*.

In primo luogo, verrà soffermata l'attenzione sulle problematiche che rappresentano una diretta conseguenza dei connotati ontologici delle nuove tecnologie, quali l'opacità in tutte le sue declinazioni e la viscerale dipendenza che sussiste tra gli *output* generati dai *tools* dalla qualità nonché attendibilità dei *big data* utilizzati.

L'analisi proseguirà verificando il rapporto che sussiste tra le nuove tecnologie e i diritti fondamentali, passando in rassegna le diverse ipotesi di violazioni degli stessi ad opera delle macchine alla luce dello studio "*Algorithms and Human rights"* commissionato nel 2016 dal Consiglio d'Europa ad un comitato di esperti.

La seconda parte del terzo capitolo sarà dedicata all'analisi delle iniziative europee e nazionali che testimoniano un'adesione sempre maggiore alla cultura della *cybersecurity* in quanto orientate a prevedere i rischi derivanti dall'utilizzo delle tecnologie di intelligenza artificiale nonché a positivizzare gli *standard* che attestino l'attendibilità ed il corretto funzionamento dei *software* impiegati a vario titolo.

Il terzo ed ultimo capitolo si concluderà verificando i diversi profili di responsabilità ascrivibili agli amministratori dell'ente e alla persona giuridica qualora si verifichi un *algorithmic misconduct*, vale a dire nel momento in cui la macchina commetta un errore idoneo ad integrare una delle fattispecie criminose tassativamente elencate nel decreto 231 del 2001.

Verrà chiarito, in *primis*, come responsabilizzare il soggetto apicale che ha scelto di avvalersi dello strumento digitale viziato nella strategia di *compliance*, per poi verificare in che modo una condotta scorretta ad opera del *tool* possa influenzare la configurazione del duplice criterio di imputazione oggettiva e soggettiva rispettivamente disciplinati agli articoli 5, 6 e 7 del decreto di riferimento.

L'ultimo tema passato in rassegna dal presente lavoro di ricerca avrà ad oggetto la disciplina vigente in materia di controlli interni a seguito della riforma entrata in vigore nel 2015. I controlli datoriali nei confronti dei sottoposi rappresentano, infatti, una delle principali attività esercitabili avvalendosi dei nuovi paradigmi digitali ed è per questo motivo che si ritiene necessario verificare in che modo la disciplina in materia si concili con quella dedicata alla *compliance* e quali siano i profili di responsabilità ascrivibili all'ente in presenza di una violazione della stessa.

CAPITOLO I

NUOVE TECNOLOGIE E DIRITTO PENALE: UN INQUADRAMENTO GENERALE FUNZIONALE ALL'INDAGINE

1. La *Digital criminal compliance*

Con il d.lgs. 231/2001, intitolato «Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica», il Governo ha dato attuazione alla delega contenuta nell'art. 11 della l. n. 300 del 200 di ratifica ed esecuzione degli accordi internazionali sulla lotta alla corruzione e alle frodi a danno degli interessi finanziari delle Comunità europee[1].

Il decreto è da annoverare tre le più rilevanti e profonde innovazioni del nostro sistema sanzionatorio[2] in quanto ha consentito il superamento del brocardo *societas delinquere non potest*, introducendo per la prima volta la diretta responsabilità da reato dell'ente[3].

Il d.lgs. n. 231 del 2001 congegna, in oltre novanta articoli, un vero e proprio "microcosmo normativo" dedicato alle persone giuridiche che consta di due parti, una di natura sostanziale e l'altra di natura procedurale, le quali presentano un diverso grado di autonomia e indipendenza dai rispettivi testi normativi dedicati alle persone fisiche[4].

---

[1] Cfr., LATTANZI, SEVERINO, *Responsabilità da reato degli enti*, vol. I, Torino, 2020, 72.

[2] Sul punto v. ALESSANDRI, *Note penalistiche sulla nuova responsabilità delle persone giuridiche*, in *Riv. Trim. dir. pen. econ*., 2002, 33.

[3] Già negli anni Settanta del secolo scorso autorevole dottrina sottolineava la necessità di introdurre una responsabilità penale degli enti, sul punto BRICOLA, *Il costo del principio "societas delinquere non potest" nell'attuale dimensione del fenomeno societario*, in *Riv. It. Dir. Proc. Pen*., 1970, 951 ss.

[4] Se la parte sostanziale è stata pensata dal legislatore italiano come un vero e proprio sottosistema normativo autonomo, la componente di natura procedurale non è completa in quanto non contiene la disciplina di tutti gli aspetti del procedimento penale in capo all'ente. Per colmare le lacune del decreto si applicano le norme del codice di procedura penale in quanto compatibili ex. art. 34, d.lgs. n. 231/2001.

La componente di natura sostanziale è suddivisa a sua volta in una parte generale[5], che ospita la disciplina dei principi generali, dei criteri di attribuzione della responsabilità, delle sanzioni, e in una parte speciale[6][7] che contiene l'elenco tassativo dei reati presupposto idonei, in presenza degli altri elementi costitutivi[8], a configurare una responsabilità in capo all'ente.

La componente procedurale del decreto, dopo aver identificato le disposizioni generali applicabili[9] ed aver eletto, in un'ottica garantista, il procedimento penale quale sede dell'accertamento della responsabilità da reato[10], disciplina sia la parte statica[11] che la parte dinamica dello stesso[12].
Dopo questa doverosa introduzione alla trattazione, è utile fornire una definizione compiuta dei tre elementi sintattici che compongono il titolo di questo primo paragrafo: il sostantivo *compliance* e i due attributi che lo accompagnano, *criminal* e *digital*.

C*ompliance* è un'espressione propria della lingua anglosassone che può essere tradotta con il termine conformità. Una parola tanto generica quanto versatile da essere in grado di compendiare diversi significati a seconda del contesto di riferimento[13]. Volendone dare una definizione onnicomprensiva, è possibile affermare che la stessa stia ad indicare l'insieme variegato di misure organizzative[14] adottate da un ente al fine di scongiurare il rischio di non conformità a regole, divieti, principi e linee

[5] V. artt. 1-23, d.lgs. 231 del 2001
[6] Si fa riferimento agli artt. 24-25 *quinquiesdecies*, d.lgs 231 del 2001
[7] La parte speciale è oggetto di continui aggiornamenti da parte del legislatore, l'ultima integrazione risale al 23 marzo 2022, data di entrata in vigore la l. n. 9 del 2022 che ha introdotto al novero dei reati presupposti gli articoli 25-*septiesdecies* e 25-*duodevicies*, rubricati rispettivamente "Delitti contro il patrimonio culturale" e "Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici".
[8] L'illecito attribuibile all'ente si configura come una fattispecie giudiziale complessa, non basta pertanto l'integrazione di uno dei reati presupposto, è necessario altresì che quest'ultimo sia stato commesso dai uno dei soggetti in posizione apicale nell'organico dell'ente ovvero dai sottoposti in caso di inosservanza degli obblighi di direzione e di vigilanza da parte dei vertici, nell'interesse o a vantaggio dell'ente, Cfr., LATTANZI, SEVERINO, *Responsabilità da reato degli enti*, Vol. II, Torino, 2020, 8.
[9] Disciplina contenuta ex art. 34, d.lgs 231/2001
[10] V. art 35, d.lgs 231/2001
[11] Si rimanda agli artt. 36-54, d.lgs 231/2001
[12] Si fa riferimento agli artt. 55-79, d.lgs. 231/2001
[13] Sul punto v., MONGILLO, *Presente e futuro della compliance penale*, in *Sist. pen*., 2022, 1 s.
[14] In argomento v., MONGILLO, *Presente e futuro*, cit., 1.

guida, sottraendosi in questo modo all'irrogazione delle sanzioni che ne derivano[15].

La *compliance* ha rappresentato una delle maggiori innovazioni degli ultimi anni in ogni suo ambito di applicazione. Se declinata al contesto aziendale, quest'ultima ha contribuito alla modifica delle strategie organizzative e di controllo interne agli enti, ora improntate alla prevenzione del rischio di violazione di disposizioni di legge e codici di condotta. In ambito penalistico, la c.d. *criminal compliance* rappresenta il fulcro di ogni strategia di contrasto alle fattispecie criminose che trovano terreno fertile nelle organizzazioni complesse[16].

A conferma di quest'ultimo aspetto sta il ruolo di assoluta centralità che la stessa riveste nel sistema normativo delineato dal d.lgs. 231/2001 sia *ex ante*, in merito alla conformazione dell'illecito, che *ex post*, in relazione alle misure riparative che l'ente ha la possibilità di adottare dopo l'integrazione della fattispecie criminosa[17].

L'importanza conferita alla stessa costituisce una peculiarità del nostro ordinamento nonché elemento di differenziazione con i modelli di responsabilità da reato degli enti adottati negli altri Paesi[18]. Nel sistema nordamericano, sia che si faccia riferimento alla *vicarious liability*[19] che *all'identification theory*[20], i *compliance programmes* non rappresentano mai un elemento costitutivo della responsabilità da imputare all'ente. Questi

[15] Cfr., NISCO, *Riflessi della compliance digitale in ambito 231*, in *Sist. pen*., 2022, 1.
[16] Sul punto v., MONGILLO, *Presente e futuro*, cit., 1.
[17] Così GULLO, *I modelli organizzativi*, in LATTANZI, SEVERINO (a cura di), *Responsabilità da reato*, vol. I, cit., 241; MONGILLO, *Presente e futuro*, cit., 3.
[18] In argomento v. SABIA, *Responsabilità da reato degli enti e paradigmi di validazione dei modelli organizzativi*, Torino, 2022, 61 ss.
[19] Si tratta di un modello di responsabilità affermatosi negli USA nei primi anni del 1900 che compendia un meccanismo di imputazione della responsabilità dal dipendente, il *servant*, al titolare dell'impresa, il *master*. È una forma di responsabilità di tipo oggettivo e indiretta (*respondeat superior*), che si applica a casi di *strict liability*, ovvero fattispecie per le quali non si richiede sussistenza di una *mens rea*, sul punto v., DE SIMONE, *Profili di diritto comparato*, in LATTANZI, SEVERINO (a cura di), *Responsabilità da reato*, vol. I, Torino, 2021, 5 s.
[20] Un modello di responsabilità che si consolida negli anni '40 del 1900 nei paesi anglosassoni e si applica in ipotesi di reato che prevedono la sussistenza dell'elemento soggettivo (*mens rea*) quale elemento costitutivo della fattispecie criminosa. Nel modello in questione, una *corporation* potrà essere ritenuta responsabile solo per atti e decisioni posti in essere da esponenti del *management* e non anche per quelli compiuti da semplici lavoratori, in argomento v., DE SIMONE, *Profili di diritto comparato*, in LATTANZI, SEVERINO (a cura di), *Responsabilità da reato*, vol, I, cit., 6 ss.

ultimi assumono un ruolo soltanto *ex post*, nello stabilire il *quantum* di pena da irrogare[21].

Anche in reazione agli accordi di *deferred* e di *non prosecuton,*[22]*,* i programmi di *compliance* vengono in rilevo soltanto quale fattore in grado di incidere sulla possibilità e sui termini dell'accordo con il *prosecutor*. L'obiettivo che si intende perseguire facendo leva su tali tipologie di accordi consiste, infatti, nel motivare l'ente ad organizzarsi quantomeno dopo la commissione del reato, definendo il procedimento tramite una soluzione negoziata[23].

La rilevanza dei *compliance programmes* in Italia, così come in Spagna ed America Latina[24], risulta pertanto decisamente più incisiva[25]. Questa scelta si giustifica alla luce delle radici in cui affonda la criminalità d'impresa. Quest'ultima scaturisce, infatti, non tanto dalle operazioni poste in essere dalle singole persone fisiche, quanto dall'articolata realtà strutturale interna alle organizzazioni a struttura complessa. L'impresa, pertanto, a causa della ripartizione orizzontale delle competenze, del decentramento delle funzioni, della frammentazione dei processi decisionali e delle asimmetrie informative, viene a porsi come contesto criminogeno idoneo a favorire il compimento dei reati presupposto[26].

In aggiunta, la stessa complessità che caratterizza l'apparato organizzativo interno alle *corporates* contribuisce a rendere difficile

[21] La valutazione dei *compliance programmes* compete al giudice. Quest'ultimo assegna all'ente uno *score* alla luce della sua colpevolezza, in applicazione delle *Federal Sentencing Guidelines* del 1991. Così GULLO, *I modelli organizzativi*, in LATTANZI, SEVERINO, *Responsabilità da reato degli enti*, vol. I, Torino, 2020, 242; COLACURCI, *L'illecito "riparato dell'ente",* Torino, 2022, 123 ss.

[22] Gli accordi di *non prosecution e deferrend prosecution* si diffondono negli Usa a partire dagli anni '70 del Novecento. Questi ultimi consistono nella valutazione dei *compliance programmes* congiuntamente ad altri elementi quali la procedura di *self reporting*, la *cooperation*, un'eventuale riorganizzazione dell'ente *ex post* e così via. La ratio dei suddetti accordi consiste nell'incentivare l'ente ad organizzarsi in modo da prevenire il reato. Per approfondimenti a riguardo si veda MAZZACUVA, *La diversione processuali per gli enti collettivi nell'esperienza anglo-americana. Alcuni spunti* de iure condendo, in *Dir. Pen. Cont. – Riv. Trim.*, 2016, 80 ss.

[23] Quello che viene valutato è come l'ente reagisce dopo aver integrato una fattispecie criminosa, la c.d. *reactive fault*

[24] Il sistema normativo delineato nella 231 ha rappresentato un modello virtuoso da seguire per gli altri paesi del mondo, quali Spagna e America Latina.

[25] Sul punto v. SABIA, *Responsabilità da reato degli enti e paradigmi di validazione,* cit., 9 ss.

[26] Sul punto v., DE SIMONE, *Profili di diritto comparato*, in LATTANZI, SEVERINO (a cura di), *Responsabilità da reato*, vol. I, cit., 59 s.

l'accertamento delle responsabilità personali dei singoli a garanzia di un'impunità generale: quel che ne deriva è un ambiente propenso alla criminalità e connotato da una c.d. «responsabilità diffusa»[27].

Il legislatore del 2001 ha scelto, pertanto, di rendere l'elemento organizzativo il fulcro della strategia normativa delineata dal decreto[28], conferendo maggiore importanza all'adozione da parte dell'ente di un modello idoneo a prevenire i reati presupposto nonché alla sua capacità di riorganizzarsi in un momento successivo, piuttosto che concentrarsi sulla punizione dello stesso. I modelli organizzativi, a cui sono dedicati gli artt. 6 e 7 del d.lgs. 231/2001[29], rappresentano «l'architrave»[30] del sistema di responsabilità degli enti.

Resta da definire l'attributo *digital.* In informatica con lo stesso si fa riferimento a tutti i dispositivi capaci di "trattare grandezze sotto forma numerica"[31], da contrapporre all'aggettivo analogico. Se affiancato al sostantivo *compliance* sarà quindi volto ad indicare l'insieme degli strumenti tecnologici messi in campo nella predisposizione di modelli organizzativi e misure di controllo interno, più in generale, idonei a prevenire i reati nel contesto dell'impresa[32], con l'obiettivo di perfezionarli, accrescerne le potenzialità e renderli più prestanti a conseguire il risultato per il quale sono pensati.

Il fenomeno della *Digital criminal compliance* sarà oggetto di un'analisi specifica da parte del seguente lavoro di ricerca. L'obiettivo è quello di verificare se l'utilizzo dei nuovi paradigmi digitali nella predisposizione di un modello organizzativo rappresenti una valida strategia per incrementare l'idoneità dello stesso a prevenire le fattispecie criminose contemplate dal decreto 231 del 2001.

---

[27] Cfr., MAGLIE, *L'etica e il mercato. La responsabilità penale delle società*, Roma, 2002, 274.
[28] Così, in particolare, MONGILLO, *Presente e futuro*, cit., 2.
[29] Un approfondimento in merito ai modelli sarà dedicato del secondo capitolo del presente contributo
[30] V. GULLO, *I modelli organizzativi*, in LATTANZI, SEVERINO (a cura di), *Responsabilità da reato degli enti*, vol. I, Torino, 2020, 242.
[31] V. *https://www.treccani.it/vocabolario/digitale2/*
[32] In argomento v. BURCHARD, *Digital Criminal Compliance*, in ENGELHART, KUDLICH, VOGEL (a cura di), *Digitalisierung, Globalisierung und Risikoprävention. Festschrift für Ulrich Sieber*, Berlino, 2021, 741; NISCO, *Riflessi della compliance*, 2022, cit., 2 s;

Per dare una risposta compiuta al seguente interrogativo si ritiene necessario esordire fornendo una panoramica dei principali strumenti digitali disponibili al giorno d'oggi, focalizzando l'attenzione sui paradigmi di intelligenza artificiale. È solo attraverso l'analisi delle caratteristiche maggiormente identificative e delle modalità di funzionamento che risulta possibile comprendere se e come avvalersi degli stessi a supporto della *compliance* penale.

2. Intelligenza artificiale (IA): definizione e caratteristiche principali

L'intelligenza artificiale sta assumendo un ruolo sempre più da protagonista in quella che non è iperbolico chiamare «rivoluzione tecnologica»[33], un processo trasformativo che coinvolge ogni ambito della realtà da un cinquantennio a questa parte. Gli anni Venti del XXI secolo, in particolare, si aprono nel contesto di un grande cambio di paradigma tecnologico, si assiste infatti ad un'evoluzione necessaria dell'informatica[34] che viene a configurarsi come supporto indispensabile per il compimento di innumerevoli attività.

L'intelligenza artificiale, alla luce delle sue potenzialità e applicazioni pratiche, viene considerata una «*disruptive technology*»[35] poiché, al pari dei *computer* e di *Internet*, genera un effetto trasformativo capace di influenzare ogni settore della vita sociale, giustizia e diritto inclusi, ed inoltre dimostra di essere il più utile degli strumenti da sfruttare per implementare la rivoluzione tecnologica in atto [36].

I principali beneficiari dell'IA risultano essere le organizzazioni complesse. A queste ultime si prospetta infatti la possibilità di sfruttare questi nuovi paradigmi tecnologici in molteplici ambiti quali, in particolare,

---

[33] Sul tema v. LAGHI, TELITI, *Processo, processi e rivoluzione tecnologica*, Padova, 2022, 1.

[34] Sul punto si veda l'intervista rilasciata da Alessandro Curioni, uno dei massimi esperti italiani di intelligenza artificiale: *https://www.agi.it/cronaca/alessandro_curioni_intelligenza_artificiale-4684053/news/2018-11-30/*

[35] Cosi nel *report* a cura del MCKINSEY GLOBAL INSTITUTE, *Disruptive technologies: Advances that will transform life, business, and the global economy*, 2013, 1 e 18.

[36] In argomento v. CALIFANO, *Ecosistemi digitali, Trasformazioni sociali e rivoluzione tecnologica XXII edizione dei Colloqui internazionali di Cortona*, in *Fondazione Giacomo Fetrinelli*, Milano, 2019, 10 ss.

il miglioramento dei sistemi produttivi, la gestione delle risorse umane, l'organizzazione della *supply chain* e, come si intende dimostrare nel presente contributo, la prevenzione del rischio di commettere reati nel contesto aziendale[37] .

Uno dei primi studi scientifici in materia di intelligenza artificiale risale alla metà del secolo scorso ed è attribuibile ad Alan Turing[38]. L'illustre matematico e logico britannico ha per primo contemplato la possibilità astratta di introdurre una macchina pensante. Il suo contributo in materia non si è limitato al solo ambito teorico, il padre putativo dell'IA, infatti, per dare attuazione pratica a quanto teorizzato, ha introdotto l'omonimo test[39] con lo scopo di verificare in termini operativi quando una macchina potesse essere considerata intelligente.

La paternità della locuzione *Artificial Intelligence*, tuttavia, non è attribuibile a Turing. L'espressione è stata utilizzata per la prima volta nel 1956 da un gruppo di studiosi[40] in occasione dell'evento *Dartmouth Summer Research Project on Artificial Intelligence*[41]. Nella dichiarazione di intenti[42] pronunciata dagli organizzatori del *workshop*, veniva affermato con convinzione che ogni aspetto dell'apprendimento e ogni manifestazione dell'intelligenza fosse passibile di una descrizione così puntuale e dettagliata da consentire ad una macchina di simularlo. Il risultato al quale ambivano gli studiosi consisteva nella progettazione di una macchina capace di usare il linguaggio, partorire ragionamenti e risolvere problemi fino a quel momento riservati esclusivamente alla competenza degli esseri umani.

---

[37] Sul punto v., SABIA, *Artificial intelligence and environmental criminal Compliance*, in ESPINOZA DE LOS MONTEROS DE LA PARRA, GULLO, MAZZACUVA (a cura di), *The Criminal Law Protection of our Common Home*, Roma, 2019, 179.

[38] Alan Turing è stato il primo studioso a chiedersi se una macchina fosse in grado di pensare, ponendosi l'ormai celebre quesito "*Can a machine think*?", cfr. TURING, *Computing Machinery and Intelligence*, in *Mind*, 1950, 1 ss.

[39] Il Test di Turing si fonda sul gioco dell'*imitation game*, per approfondimenti al riguardo v. LONGO, *Il test di turing storia e significato*, in *Mondo Digitale*, 2009, 2 ss.

[40] John McCarhty, Marvin Minsky, Claude Shannon e Nathaniel Rochester

[41] In argomento v., ITALIANO, *Intelligenza Artificiale: passato, presente, futuro*, in PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, 208 ss.

[42] Per approfondimenti al riguardo si veda: MCCARTHY, MINSKY, ROCHESTER, SHANNON, *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, in *AI Magazine*, 2006, 12.

Dall'occasione di conio della locuzione ad oggi sono stati fatti notevoli passi in avanti. Il dato più significativo è che al giorno d'oggi le tecnologie di IA sono presenti in maniera diffusa nella vita di tutti i giorni, basti pensare al loro utilizzo per tradurre automaticamente da una lingua all'altra, per riconoscere discorsi, per effettuare pianificazioni logistiche, per contrastare *e-mail spam* e così via[43]. Risulta che i notevoli progressi in materia non siano tanto dovuti ad un mutamento delle tecniche impiegate, che sono in larga parte simili a quelle già teorizzate in passato, quanto alla disponibilità di una potenza di calcolo notevolmente superiore nonché alla presenza al giorno d'oggi di un enorme quantità di dati da sfruttare[44].

All'alto livello di tecnicismo raggiunto negli ultimi anni non corrisponde altrettanta chiarezza definitoria in materia. Non esiste ancora una definizione ufficiale e condivisa di Intelligenza artificiale[45] pertanto, ai fini della trattazione, è utile illustrare le tre più autorevoli seguendo l'ordine cronologico in cui sono state rese pubbliche.

Il primo contributo definitorio che sembra opportuno menzionare è quello contenuto nel glossario in coda alla Carta Etica Europea[46]. Quest'ultimo descrive l'intelligenza artificiale come un insieme di metodi, teorie e tecniche scientifiche che consentono ad una macchina di riprodurre le capacità cognitive degli esseri umani. L'obiettivo che gli esperti in materia di nuove tecnologie intendono perseguire consiste quindi nel programmare un *software* capace di sostituirsi all'uomo, in modo da poter delegare allo stesso una serie di compiti più o meno complessi che fino a questo momento potevano essere portati a termine soltanto dallo stesso.

Più specifica risulta essere la definizione contenuta nel documento elaborato da un Gruppo Indipendente di esperti in materia di intelligenza

[43] Sul tema v., RUSSEL, NORVIG, *Artificial Intelligence – A modern approach*, ed. III, Londra, 2010, 29.
[44] Cfr. ITALIANO, *Intelligenza Artificiale: passato, presente, futuro,* cit., 218.
[45] In argomento v. NISCO, *Riflessi della compliance digitale*, cit., 3.
[46] La Carta etica europea è stata adottata dalla Commissione europea per l'efficacia della giustizia (CEPEJ) il 4 dicembre 2018. Il testo integrale è disponibile sul sito ufficiale del Consiglio d'Europa consultabile al seguente link: *https://www.coe.int/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment*

artificiale nominato dalla Commissione Europea[47] nel 2018 perché, a differenza di quella poc'anzi riportata, entra nel merito del funzionamento della tecnologia in esame.

I sistemi di IA vengono descritti come *software* progettati dall'uomo in modo tale da renderli capaci di conseguire un obiettivo previamente definito e di operare sia nella sfera fisica che in quella digitale. Si precisa che la percezione della realtà da parte del *software* è resa possibile grazie all'acquisizione, allo studio e all'interpretazione dei dati: un'attività che viene considerata propedeutica alla scelta della soluzione ideale da adottare per conseguire al meglio il *task* assegnato in sede di programmazione. Si sottolinea ulteriormente che, nell'operazione di selezione del miglior approccio possibile, i sistemi di intelligenza artificiale si avvalgono di regole simboliche o modelli numerici e, se programmati adeguatamente, sono capaci di adattare il loro comportamento futuro alla realtà circostante e ai continui cambiamenti che la stessa subisce, anche per effetto delle azioni poste in essere in precedenza.

La definizione cronologicamente più recente di IA è quella contenuta nell'art. 3 della Proposta di regolamento europeo avanzata in data 21 aprile 2021 da parte del Parlamento europeo e del Consiglio[48]. Il provvedimento normativo in questione descrive l'intelligenza artificiale come *software* progettato con il contributo di una o più delle tecniche e degli approcci elencati nell'allegato I allo stesso regolamento[49]. Si tratta di un *tool* idoneo a generare *output* quali contenuti, previsioni, raccomandazioni o

[47] Il report "*A definition of AI: Main Capabilities and Disciplines*" elaborato nel 2019 *dall'High-Level Expert Group* è disponibile sul sito ufficiale della Commissione europea: *https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines*

[48] Sul punto v. COMMISSIONE EUROPEA, *Proposta di regolamento del parlamento europeo e del consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione commissione europea*, Bruxelles, 2021 COM(2021) 206 *final*, art. 3.

[49] L'allegato I menziona gli approcci di apprendimento automatico, compresi l'apprendimento supervisionato, l'apprendimento non supervisionato e l'apprendimento per rinforzo, con utilizzo di un'ampia gamma di metodi, tra cui l'apprendimento profondo (*deep learning*); approcci basati sulla logica e approcci basati sulla conoscenza, compresi la rappresentazione della conoscenza, la programmazione induttiva (logica), le basi di conoscenze, i motori inferenziali e deduttivi, il ragionamento (simbolico) e i sistemi esperti; approcci statistici, stima bayesiana, metodi di ricerca e ottimizzazione.

decisioni che influenzano gli ambienti con cui interagiscono, tutti orientati al conseguimento di un range di obiettivi previamente definiti dall'uomo[50].

Un utile contributo volto a rendere più organici i contributi scientifici e normativi in materia è da attribuire al Servizio Scienza e conoscenza della Commissione europea[51]. Nell'ambito del progetto finalizzato alla creazione di un mercato unico digitale, la Commissione ha infatti presentato una strategia unica europea concernente l'IA[52] al fine di conseguire una serie di risultati a livello comunitario[53].

Il Centro di ricerca ha svolto in *primis* un'indagine completa sulle diverse definizioni di IA sviluppatesi finora ed ha portato a termine un lavoro di sintesi tra le stesse, proponendone una operativa, composta da un insieme di parole chiave che caratterizzano i domini centrali e trasversali dell'IA[54].

L'esito dello studio individua, inoltre, in quattro caratteristiche ricorrenti il minimo comun denominatore tra la moltitudine di definizioni di IA diffusesi negli anni. Risulta infatti che ogni sistema di IA si basi sulla considerazione della complessità del mondo reale, che operi attraverso

---

[50] La Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale e modifica alcuni atti legislativi dell'Unione è disponibile sul sito ufficiale dell'Unione Europea: *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32021R0694&qid=1678716870708*. Per un approfondimento sul tema si rimanda al paragrafo 4 del presente contributo.

[51] Si tratta del Centro di ricerca che fornisce consulenze scientifiche e opera come centro di diffusione della conoscenza nell'interfaccia tra scienza e politica. Per saperne di più al riguardo si consulti la pagina ufficiale dell'Ufficio delle pubblicazioni dell'unione europea: *https://op.europa.eu/it/publication-detail/-/publication/c782d6c7-33f7-11e9-8d04-01aa75ed71a1*

[52] Secondo quanto stabilito nella comunicazione "*Artificial Intelligence for Europe*" COM(2018)237, aprile 2018, per "intelligenza artificiale" (IA) si intendono «quei sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere obiettivi specifici. Usiamo l'IA quotidianamente, ad esempio per bloccare lo spam nella posta elettronica o per parlare con gli assistenti digitali. L'aumento della potenza di calcolo e della disponibilità dei dati e il progresso negli algoritmi hanno reso l'IA una delle tecnologie più importanti del 21° secolo».

[53] Gli obiettivi da conseguire con la strategia vengono enunciati nel preambolo della stessa. Si intende in primo luogo rafforzare le capacità tecnologiche e industriali dell'Unione Europea mediante l'impiego dei sistemi di intelligenza artificiale in ogni settore economico, in secondo luogo, acquisire consapevolezza circa i cambiamenti socioeconomici quale immediata conseguenza dell'utilizzo delle nuove tecnologie ed in ultimo elaborare una cornice etica e giuridica adeguata.

[54] I risultati dell'indagine sono contenuti nel report a cura del JCR TECHNICAL REPORTS, *AI Watch: Defining Artificial Intelligence. Towards an operational definition and taxonomy of artificial intelligence, https://op.europa.eu/en/publication-detail/-/publication/83838dbc-3d1f-11ec-89db-01aa75ed71a1/language-en accessed 28 August 2021.*

l'elaborazione di informazioni, che sia finalizzato al raggiungimento di obiettivi specifici e che presenti un alto livello di autonomia nel ragionare, apprendere, decidere ed operare.

È quest'ultimo l'aspetto più innovativo della tecnologia in questione, ovvero la capacità di autodeterminarsi, elaborando una mole enorme di dati in tempi estremamente ridotti e, soprattutto, senza limitarsi a riprodurre schemi decisionali preimpostati, bensì adottando scelte operative che non richiedono l'intervento umano, tanto da propendere a definirli "intelligenti"[55].

E ancora, la dottrina, sempre al fine di raggiungere un livello minimo di accordo tra le teorie che sia avvicendano, riconosce quali caratteristiche comuni a tutte le declinazioni di intelligenza artificiale l'impiego di grandi quantità di dati e informazioni, l'elevata capacità logico-computazionale e l'uso di nuovi algoritmi idonei a ricavare informazioni utili dall'analisi della mole di dati a disposizione, così da conferire alle macchine la capacità di prendere decisioni corrette negli ambiti più disparati[56].

Le evidenti difficoltà definitorie sono in parte giustificate dalla moltitudine di sfaccettature di IA esistenti, tanto che talvolta si è preferito parare di «Intelligenze artificiali» al plurale piuttosto che al singolare[57]. Lo stesso Gruppo indipendente di esperti evidenzia come l'IA includa diversi approcci e tecniche[58], come il *machine learning*, il *machine reasoning* e la *robotic*.

Una prima fondamentale classificazione all'interno della macrocategoria di IA riguarda l'intelligenza artificiale in senso forte, c.d. *Strong AI*, e l'intelligenza artificiale in senso debole, c.d. *Weak AI* [59].
L'intelligenza artificiale in senso forte mira a ricostruire nelle macchine un livello di intelligenza pari a quello dell'uomo. I *software*, nella maggior

[55] Sul punto v. NISCO, *Riflessi della compliance digitale*, cit., 3.
[56] In argomento v. UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in *Riv. Dir. pen. cont.*, 2020, 77.
[57] Sul tema v., CASONATO, *Giustizia e intelligenza artificiale: considerazioni introduttive*, in *BioLaw Journal – Riv. di BioDiritto*, 2021, 359.
[58] Cfr., HIGH-LEVEL EXPERT GROUP, *A definition of AI: Main Capabilities and Disciplines*, 2019, 3 ss.
[59] A tal riguardo v., SEARLE, *Minds, Brains and Programmes*, Londra, 1980, 1 ss.

parte dei casi incorporati ad *hardware*, non vengono a configurarsi come meri strumenti utili alla mente umana ma, se adeguatamente programmati, saranno essi stessi, ontologicamente parlando, una mente[60] dotata di una capacità cognitiva non dissimile da quella umana.

Questa teoria in virtù della quale anche un *tool* sarebbe in potenza capace di conoscere e comprende, tanto da essere assimilabile ad un cervello, affonda le proprie radici nella concezione di intelligenza quale insieme di calcoli della mente umana[61]. È proprio nella *strong AI* che è ravvisabile l'idea originaria del padre putativo dell'intelligenza artificiale, Alan Turing, il cui progetto originario consisteva nel riprodurre una macchina *human-like*, dotata di un'intelligenza ad ampio spettro[62].

Entrando nel merito del funzionamento dell'intelligenza nella sua accezione forte, risulta che la tecnologia alla base della stessa sia quella dei sistemi esperti, vale a dire programmi *software* capaci di riprodurre le prestazioni e le conoscenze delle persone esperte in un determinato campo di applicazione, anche detto dominio, e di sostituirsi in tutto e per tutto all'essere umano[63].

Le ambizioni a tratti utopiche dei primi teorici in materia sono state progressivamente ridimensionate negli anni successivi, tanto che si è deciso di concentrare gli sforzi nella costruzione di sistemi capaci di operare "intelligentemente" nell'ambito di un più ristretto dominio, abbandonando l'idea di un'intelligenza artificiale a portata generale.

---

[60] Un approccio critico sul punto è fornito da Searle. Quest'ultimo, attraverso la sua argomentazione nota come la "Stanza Cinese", esclude che una macchina, seppur capace di superare il Test di Turing, possa essere considerata intelligente al pari di un umano, v. SEARLE, *Minds, Brains*, cit., 3 ss.

[61] Il filosofo Thomas Hobbes (1588-1679), sulla scia di quanto teorizzato secoli prima da Aristotele, ha paragonato il ragionamento umano ad un insieme di calcoli ed operazioni matematiche. Per un approfondimento sul punto v. RUSSEL, NORVIG, *Artificial Intelligence*, cit. 1 ss.

[62] L'obiettivo che era da considerarsi raggiunto qualora il tool fosse in grado di superare il *Test* di Turing, basato interamente sul gioco dell'imitazione.

[63] Questi ultimi constano di tre livelli tecnologici diversi, il primo dei quali è rappresentato dalla c.d. base di conoscenza o knowledge base, un *database* dove vengono immagazzinate le informazioni e le regole di cui il sistema necessita per operare, il secondo elemento strutturale consiste nel motore inferenziale, un *set* di indicazioni di tipo "*if-then*" che indirizza il sistema nella scelta del miglior comportamento da attuare a seconda del contesto specifico ed in ultimo la c.d. interfaccia utente, ovvero la componente software che garantisce un'interazione tra macchina ed essere umano e consente a quest'ultimo di avvalersi del motore inferenziale. Per saperne di più sul punto v. *https://www.ai4business.it/intelligenza-artificiale/sistemi-esperti-cosa-sono/*

Nasce così l'altra tipologia di IA, la c.d. intelligenza artificiale in senso debole, anche chiamata *narrow AI.* Con tale denominazione si fa riferimento a quegli algoritmi capaci di concorrere con l'uomo in compiti specifici, dando solo l'impressione di essere effettivamente pensanti. L' obiettivo dei ricercatori in materia di IA debole non consiste, infatti, nel realizzare *software* intrinsecamente dotati di un'intelligenza a tutto campo, quanto nel progettare sistemi che siano in grado di simulare un determinato comportamento umano, senza la pretesa di eguagliarlo o addirittura emularlo [64].

L'"intelligenza" di tali paradigmi tecnologici è ravvisabile nella capacità di sostituirsi all'uomo nello svolgimento di un compito specifico, nell'abilità di affrontare e risolvere un problema nuovo e nell'idoneità a migliorare i processi decisionali nei settori in cui sono utilizzati [65].

Gli ultimi approdi scientifici nel campo delle nuove tecnologie consentono di programmare software non ancora del tutto svincolati dalla presenza dell'uomo e quindi appartenenti a questa seconda declinazione di intelligenza artificiale. La creazione di algoritmi di IA forte viene pertanto concepita come un obiettivo a lungo periodo, bisognoso di ulteriori studi e sperimentazioni sia a livello teorico che pratico [66].

Evidenze concrete di intelligenza artificiale nell'accezione debole verranno illustrati nei due sottoparagrafi che seguono.

2.1 Big Data analysis

In virtù delle nuove tecnologie dell'informazione e della comunicazione, nel corso dell'ultimo ventennio si è passati da un c.d. società dell'informazione[67] ad una c.d. società della conoscenza. Se la prima si limita a creare e a diffondere dati grezzi, la seconda è finalizzata a

[64] A tal riguardo v., SEARLE, *Minds, Brains and Programmes*, Londra, 1980, 9 ss.

[65] Sul punto vedi la Comunicazione della Commissione europea sul piano coordinato sull'intelligenza artificiale, COM/2018/795 final, pubblicata nell'aprile 2018.

[66] Sul tema v., VERMEULEN, PERŠAK, RECCHIA, *Artificial Intelligence, Big Data and Automated Decision-Making in Criminal Justice,* in *RIDP*, 2021, 110.

[67] La Società dell'Informazione è un tipo di società in cui la trasmissione di dati e informazioni svolge un ruolo preponderante sulla scena economica, culturale e politica.

trasformare le informazioni generate e raccolte in risorse utili a generare uno sviluppo nella società [68]. L'acquisizione delle stesse non è più fine a sé stessa ma serve a realizzare un obiettivo più alto e più auspicabile, vale a dire la conoscenza, fonte di sviluppo per tutti, in primo luogo per le economie globali [69].

Al fine di conseguire un livello conoscenza adeguato occorre un'ingente quantità di dati qualitativamente validi. Necessità pienamente soddisfatta, per lo meno da un punto di vista quantitativo, posto che la produzione degli stessi ha vissuto una crescita esponenziale, sembrerebbe infatti che le informazioni che circolano ogni secondo sul *web* siano pari ai dati presenti in internet 20 anni fa [70].

Questi ultimi vengono considerati il "nuovo petrolio" in virtù della loro capacità di generare ricchezza nelle nostre economie[71], obiettivo che dipende strettamente dalla capacità di analizzare, comprendere e sfruttare appieno il valore degli stessi[72].

L'analisi dei dati per produrre informazioni fruibili rappresenta pertanto una sfida chiave e un'opportunità per le imprese, in quanto lo sfruttamento adeguato di tali informazioni costituirà un elemento di differenziazione per le aziende orientate al futuro[73].

Alla luce delle predette considerazioni, è evidente quanto sia importante la tecnologia della *big data analytics*. Quest'ultima costituisce il sottoinsieme più studiato e adoperato all'interno della macrocategoria di intelligenza artificiale in senso debole. Con tale espressione ci si riferisce alla capacità propria degli algoritmi di intelligenza artificiale di estrapolare,

---

[68] In argomento v. CASTELFRANCHI, *Six critical remarks on science and the construction of the knowledge society*, in *Journal of Science Communication*, 2007, 1 e 3

[69] Così, in particolare, l' UNESCO *World Report United Nations Educational*, dal titolo *Scientific and Cultural Organization. Toward knowledge societies*, 2005.

[70] Sul punto v. BARRY, LIBERT, *Why Boards Must Embrace Big Data*, in *NACD Directorship*, 2013, 1 ss.

[71] Il mercato italiano è cresciuto del +27% nel 2021, raggiungendo il valore complessivo di 380 milioni stando a quanto riportato dal contributo pubblicato nel 2022 a cura dell'Osservatorio.net gestito dal Politecnico di Milano, *https://www.osservatori.net/it/ricerche/comunicati-stampa/artificial-intelligence-italia-mercato-progetti-2020*

[72] A tal riguardo il parere n. 7/2015 dell' EUROPEAN DATA PROTECTION SUPERVISOR, *Meeting the challenges of big data*.

[73] Si veda il rapporto di gennaio 2014 dello EY *Center for Board Matters*, p. 2 ss.: *The bar is raised: anti-corruption compliance now requires big data analytics*.

analizzare e mettere in relazione un'enorme mole di dati eterogenei, strutturati e non, al fine di individuare legami tra fenomeni diversi e prevedere quelli futuri.

Per comprendere a pieno in cosa consiste la tecnologia in questione e fornire un quadro generale circa le sue applicazioni pratiche, occorre specificare cosa si intende per *big data*.

L'espressione *big data* indica i grandi insiemi di dati provenienti da fonti miste[74], questi ultimi si caratterizzano da tre elementi principali, le c.d. «tre V», vale dire volume, varietà e velocità[75].

Per volume si intende la quantità di dati generati, memorizzati e gestiti all'interno del sistema. L'aumento dello stesso si spiega con la crescita numerica dei dati generati e archiviati, ma anche con la necessità di sfruttarne in quantità sempre maggiori[76].

Il sostantivo varietà assume una duplice accezione, si riferisce sia alle diverse tipologie di dati esistenti nel sistema[77], i quali provengono dalle fonti più disparate[78], sia alla vasta gamma di possibili usi associati ad un dato grezzo.

Quanto alle diverse declinazioni di dati presenti, ne esistono tre categorie principali di dati. In primo luogo, quelli strutturati[79], i quali rispettano un *set* di regole predeterminato tanto da poterne definirne la tipologia e le relazioni reciproche. Questi ultimi dipendono sempre da uno schema, possono essere pertanto rappresentati in righe e colonne e sono passibili di archiviazione in un *database* relazionale. In secondo luogo, i dati semi-strutturati[80]. Questi ultimi sono senza schema e rappresentabili

[74] Definizione contenuta nel Glossario della Carta Etica Europea il cui testo integrale è disponibile sul sito ufficiale del Consiglio d'Europa *https://www.coe.int/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment*

[75] È stato Gartner il primo autore a definire I big data con le tre V: volume, velocità e varietà. Per saperne di più sul punto v. ZAKIR, SEYMOUR, BERG, *Big data analytics,* in *Issues in Information Systems*, vol. XVI, 2015, 81 ss.

[76] Sul punto v. RIAHI, *Big Data and Big Data Analytics: Concepts, Types and Technologies*, in IJRE, 2018, 352.

[77] Transazioni bancarie, ordini, sondaggi, attività online, previsioni e informazioni sul traffico sono alcune delle tipologie di dati esistenti, sul tema v. EY *Center for Board Matters*, p. 2 ss.: *The bar is raised* cit.

[78] Per un approfondimento sul punto v. COSIMI, *Origine dei "Big Data"*, in *Gnosis*, 2017, 130 ss.

[79] Esempi concreti di dati strutturati sono la data, il nome e l'indirizzo

[80] Le *e-mail*, i *file* HTML e XML appartengono alla categoria dei dati semi-strutturati

attraverso etichette, grafici e strutture ad albero. In terzo luogo, i dati non strutturati[81], i quali, a differenza di quelli catalogabili nelle due categorie poc'anzi illustrate, non seguono un modello predefinito e non possono essere organizzati in righe e colonne. Questi ultimi possono avere origini molto diverse[82]: ne deriva una difficoltà nella loro comprensione e un'ambiguità nella loro collocazione. Si differenziano ulteriormente per via della loro grandezza e voluminosità, decisamente superiori rispetto ai dati strutturati.

Il terzo requisito che definisce i *big data* è la velocità, quest'ultima fa riferimento sia alla frequenza con cui i dati vengono generati, acquisiti e condivisi[83] che alla rapidità con cui evolve il loro contenuto[84].

A questa triade di elementi ne sono stati affiancati altri due, ovvero la veridicità, la quale considera il livello di qualità ed accuratezza dei dati e delle fonti da cui gli stessi derivano, ed in ultimo il valore, vale a dire il loro contributo a favore di chi se ne avvale nonché il potenziale intrinseco agli stessi.[85]

Per trarre un concreto beneficio da questo *mare magnum* di informazioni, è di fondamentale importanza saper analizzare le stesse avvalendosi del supporto di *tools* idonei a produrre intuizioni utili e nuovo valore [86]. L'analisi dei *big data* consiste proprio nell'impiego di tecniche di analisi altamente sofisticate su grandi volumi di dati, allo scopo di descrivere eventi e situazioni, identificare *pattern*, correlazioni o tendenze e trasformare così il dato grezzo in informazione utile e funzionale alla scelta della migliore soluzione al problema.

---

[81] Carenti di una struttura fissa e quindi appartenenti alla terza categoria di *big data* sono, ad esempio, immagini, audio e video

[82] Possono essere estratti da un linguaggio umano, acquisiti attraverso sensori, ricavati dai *social media*. Cfr. COSIMI, *Origine dei "Big Data"*, cit., 130.

[83] Sul punto v. RIAHI, *Big Data*, cit., 352.

[84] Il contenuto dei *big data* è in continua e rapida evoluzione in virtù, ad esempio, dell'associazione di raccolte di dati complementari, della riemersione di informazioni archiviate in un momento precedente e dello *streaming* di dati provenienti da più fonti

[85] Gartner ha ampliato la sua definizione nel 2012 per includere la veridicità e valore, cfr., v. ZAKIR, SEYMOUR, BERG, *Big data analytics*, cit., 81 ss.

[86] FERGUSON, *Big data and predictive reasonable suspicion*, in *University of Pennsylvania law review*, 2015, 351.

L'obiettivo più ambizioso della *big data analytics* è proprio quello di consentire a chi se ne avvale di prendere decisioni in maniera più rapida e consapevole. Le soluzioni scelte saranno infatti basate su dati ed informazioni concrete che, senza il contributo delle tecnologie odierne, sarebbero risultate in passato inaccessibili.

Esistono quattro principali categorie di *big data analysis*, ognuna volta a conseguire uno scopo ben preciso. La prima è denominata *decriptive analysis*[87] e rappresenta la fase preliminare nel processo di elaborazione dei dati. Il suo *task* principale è quello di distillare i dati grezzi organizzandoli e mettendoli in relazione in un formato fruibile e di facile comprensione, avvalendosi della *business intelligence* tradizionale.[88]

La seconda prende il nome di *diagnostic analysis*[89], quest'ultima viene concepita come logica prosecuzione della prima declinazione[90] in quanto consente di rintracciare e comprendere le cause che hanno determinato un dato evento, comportamento o problematica. L'analisi diagnostica può essere eseguita manualmente, utilizzando un algoritmo, o avvalendosi di *software* statistici come *Microsoft Excel*.[91]

Il terzo *step* nel processo di analisi del dato è rappresentato dalla *predictive analysis*[92], tecnologia che consente di analizzare i dati dapprima raccolti e poi ordinati, sotto al profilo delle cause generatrici. L'analisi predittiva si avvale di tecniche quali il *data mining* e l'intelligenza artificiale per generare previsioni future sulla base delle informazioni in possesso.

---

[87] Gartner definisce l'analisi descrittiva come l'esame di dati o contenuti per rispondere alla domanda "Cosa è successo?", sul punto v. RIAHI, *Big Data*, cit., 352

[88] La *business intelligence* (BI) è un *software* che acquisisce dati aziendali e li presenta in visualizzazioni intuitive come *report*, *dashboard*, diagrammi e grafici, sul tema v. *https://www.ibm.com/it-it/topics/business-intelligence*.

[89] Secondo Gartner, quella diagnostica è una forma di analisi avanzata che esamina dati e contenuti con l'obiettivo di rispondere al quesito: "Perché è successo?" Quest'ultima si avvale di tecniche quali il *drill-down*, il *data discovery* e il *data mining*, in argomento v. RIAHI, *Big Data*, cit., 525

[90] Si fa riferimento alla *descriptive analysis*

[91] Sul punto il contributo di Harvard Business School consultabile al seguente link: https://online.hbs.edu/blog/post/diagnostic-analytics

[92] L'analisi predittiva, alla luce di quanto affermato da Garner, risulta utile a rispondere alla domanda: "Cos'è probabile che accada?", cfr., RIAHI, *Big Data*, cit., 525.

La quarta ed ultima categoria di *big data analysis* è denominata *prescriptive analysis*[93]. Essa si avvale dei parametri generati nelle tre fasi precedenti per stabilire l'azione giusta da intraprendere, la soluzione migliore al problema o la decisione più corretta da assumere. Consiste in tecniche quali l'analisi dei grafici, la simulazione, l'elaborazione di eventi complessi, le reti neurali, i motori di raccomandazione, l'euristica e il *machine learning*.

Compete al consiglio di amministrazione la scelta della migliore strategia di *Big data analysis* da adottare all'interno di un'impresa. L'organo amministrativo ha infatti il compito di assicurarsi che il CEO e il *team* di gestione abbiano adottato le misure più efficaci per lo sviluppo di un approccio strategico per l'impresa. Sono state pertanto elaborate delle *best practices*[94] utili ad orientare l'attività del CDA nell'affrontare le sfide poste dai *big data*.

La prima linea guida consiglia di stabilire a monte cosa si intende ottenere dalla raccolta e dallo sfruttamento dei dati. È preferibile, pertanto, procedere all'inverso rispetto al tradizionale *modus operandi* delle imprese, dove il dato è concepito come punto di partenza e dove ci si interroga circa i suoi impieghi e le metodologie di analisi da adottare solo in un secondo momento. Si consiglia pertanto di fare luce dapprima sulle decisioni che si devono assumere e utilizzare le informazioni a disposizione per dimostrare o confutare le ipotesi prospettate. Procedendo in quest'ordine, l'impresa eviterà che sia il dato ad orientare il processo decisionale e si concentrerà nella raccolta e nell'analisi delle sole informazioni che hanno un impatto diretto sulla decisione da assumere, il che consentirà di risparmiare energie e risorse economiche.

La seconda *best practice* consiste nel determinare sin da subito quali siano le informazioni rilevanti. Come già illustrato in precedenza, la quantità dei dati disponibili al giorno d'oggi è notevole, risulta pertanto impensabile

[93] "Cosa è opportuno che si faccia?": è questo il quesito che l'analisi prescrittiva è orientata a chiarire, alla luce di quanto sostenuto da Garner, sul punto v. RIAHI, *Big Data*, cit., 525.
[94] Si veda il rapporto di gennaio 2014 dello EY *Center for Board Matters*, p. 2 ss.: *The bar is raised* cit.

e poco proficuo raccoglierli e analizzarli tutti al fine di un loro sfruttamento in quanto gran parte degli stessi non è rilevante per le decisioni aziendali che la *corporation* deve adottare. È preferibile che le imprese abbandonino l'approccio «*no stone left unturned*»[95] per concentrarsi su una cerchia di dati più contenuta ma in grado di fare luce sul problema in questione o addirittura idonea ad anticiparne l'esistenza.[96]

La terza ed ultima indicazione pubblicata consiglia alle imprese di concentrarsi sui soli dati capaci di apportare valore alle stesse. Preso atto che la quarta "V" utile a definire i *big data* sia proprio il valore, si richiede alle società di selezionare sin da subito le informazioni capaci di apportare un concreto beneficio, ordinando i set di dati a disposizione per determinare quali abbiano maggiori probabilità di generare lo stesso. Una volta completata quest'operazione di raccolta e classificazione delle informazioni, seguirà una fase di valutazione basata su ipotesi e previsioni da verificare.

Un esempio pratico di *software* impiegato nell'analisi di ingenti quantità di informazioni fino a qualche tempo fa considerate impossibili da archiviare ed elaborare prende il nome di *Hadoop*[97]. Quest'ultimo consente l'elaborazione distribuita di grandi insiemi di dati tra *cluster* di computer, attraverso l'utilizzo di semplici modelli di programmazione ed è progettato per essere scalabile da singoli *server* a migliaia di macchine.

Hadoop è stato realizzato nonché reso disponibile gratuitamente dalla *Apache Foundation* e viene utilizzato da aziende con grandi volumi di dati da elaborare quali *Facebook, Twitter, LinkedIn, eBay* e *Amazon*[98].

[95] In questi termini il rapporto EY del 2014, p. 3. Letteralmente, "nessuna pietra lasciata irrovesciata": l'espressione figurata indica quell'approccio volto a non tralasciare nulla.

[97] Per ulteriori approfondimenti a riguardo è possibile consultare il sito ufficiale di *Hadoop*: *https://hadoop.apache.org/*

[98] Sul tema v. RIAHI, *Big Data*, cit., 526

2.2 Machine learning

Una declinazione dell'intelligenza artificiale che merita un approfondimento specifico in virtù della sua importanza nella società odierna e delle sue potenzialità per il prossimo futuro[99] è la tecnologia di *machine learning*.

Il *Machine Learning* o apprendimento automatico è una sottocategoria dell'IA debole che si occupa di studiare e programmare algoritmi[100] capaci di consentire ad un sistema di intelligenza artificiale di apprendere, come suggerisce la denominazione stessa[101]. La caratteristica che contrassegna gli algoritmi di *machine learning* e che li differenzia da quelli tradizionali consiste nella loro capacità di imparare in maniera autonoma a partire dall'osservazione dei dati messi a disposizione.

In tal senso urge una precisazione: affermare che una macchina sia capace di apprendere non significa che la stessa divenga in grado di replicare pedissequamente il complesso e articolato sistema cognitivo di pensiero proprio della mente umana[102] ma implica che tali sistemi siano capaci di migliorare la propria performance futura grazie all'osservazione della realtà[103]. In altre parole, la potenzialità propria degli algoritmi in questione consiste nel saper trarre regole comportamentali e modelli comuni attraverso l'esame e il confronto di grandi insiemi di dati.

---

[99] L'ingente quantità di dati disponibili al giorno d'oggi porta ad affermare che il *machine learning* avrà un ruolo da protagonista nella prossima ondata di innovazioni, sul punto v. DOMINGOS, *A Few Useful Things to Know about Machine Learning*, in *Communications of the* ACM, 2012, 78.

[100] Un algoritmo è un procedimento che risolve un determinato problema attraverso un numero finito di passi elementari, chiari e non ambigui: a partire da uno o più dati di *input*, produce un risultato in forma di *output*. Sul punto v. BARILLARO, *Che cos'è un algoritmo in generale e in informatica,* in *Informatica per tutti*, 2023. *https://www.informaticapertutti.com/che-cose-un-algoritmo-in-generale-e-in-informatica/*

[101] Sul punto v. HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE, *A definition of AI: main capabilities and disciplines,* 2019, 3

[102] L'obiettivo degli studi di machine learning non consiste nel progettare una macchina ontologicamente intelligente al pari dell'uomo, come invece si auspica nella concezione forte di intelligenza artificiale cfr. v., SEARLE, *Minds, Brains and Programmes*, Londra, 1980, 1 ss.

[103] WITTEN, FRANK, HALL, *Data mining. Practical Machin Learning Tools and Techniques*, Burligton, 2011, 7.

Necessario al conseguimento dell'obiettivo illustrato è l'"allenamento" o *training*[104]. In questa fase il *software* fa esperienza della realtà ed elabora delle conclusioni che andranno ad influenzare il suo comportamento successivo. Tale processo di *training* ha una durata variabile: persiste fino a quando il sistema non avrà raggiunto il livello desiderato di accuratezza in relazione agli *input* forniti. Lo scopo ultimo dello stesso, infatti, consiste nell' istruire la macchina in modo che la stessa divenga capace di effettuare previsioni, eseguire *clustering*, estrarre regole di associazione, prendere decisioni o svolgere una determinata mansione senza che sia preventivamente programmata dall'uomo.

A seconda della metodologia di *training* a cui è sottoposto l'algoritmo, è possibile distinguere tra quattro categorie principali di *machine learning*[105].

La prima declinazione di apprendimento automatico prende il nome di *machine learning* supervisionato. Si tratta della sottocategoria che mostra il maggior livello di dipendenza dal contributo umano in quanto, durante la fase di allenamento, vengono forniti sia i dati di *input* che quelli di *output* precedentemente selezionati, etichettati e classificati[106]. L'utilità maggiore della tecnologia di *machine learning* supervisionato consiste proprio nel delineare il rapporto di correlazione tra variabili tracciando una funzione che ricollega le prime alle seconde [107] I principali algoritmi su cui ci basa questa prima declinazione di *machine learning* sono di due tipi e prendono il nome di *classification* e *regression*[108].

---

[104] Questa fase consiste nella sottoposizione all'algoritmo di diversi casi pratici da parte del programmatore. Per ulteriori approfondimenti sul punto v. UÇAR, NOUR, SINDI, POLAT, *The Effect of Training and Testing Process on Machine Learning in Biomedical Datasets*, in *Hindawi, Mathematical Problems in Engineering*, 2020, 1 ss.

[105] Cfr. MOHAMMED, KHAN, BASHIER, *Machine Learning, Algorithms and Applications*, Boca Raton, 2017, 7.

[106] L'algoritmo di cui si avvale il machine learning supervisionato consta quindi di una variabile dipendente, anche detta variabile di *output*, che deriva direttamente dall'altra variabile, quella indipendente, vale a dire l'*input* fornito. Cfr., MOHAMMED, KHAN, BASHIER, *Machine Learning*, cit., 7 s.

[107] In concreto vengono sottoposti all'algoritmo degli esempi dove ad una data x ne deriva una data y, così facendo il computer viene istruito a derivare una relazione tra le variabili x e y.

[108] V. MOHAMMED, KHAN, BASHIER, *Machine Learning*, cit., 8

Nella *classification*, l'insieme dei dati grezzi vengono dapprima organizzati in specifici gruppi e in un momento successivo si illustra all'algoritmo come classificare il *set* di informazioni alla luce di una o più caratteristiche specifiche. Seguendo l'impostazione illustrata, il *tool* riuscirà a procedere autonomamente nelle operazioni di distribuzione dei dati.[109] Prende il nome di binaria la *classification* che si sostanza di due categorie, mentre la stessa viene denominata *multi-label* quando i gruppi di classificazione sono più di due. [110]

La *regression* è l'altra tecnica di apprendimento supervisionato. Ci si avvale della stessa per ricavare correlazioni tra le variabili e fare predizioni alla luce delle informazioni di cui si è a conoscenza. Si distingue ulteriormente tra *simple linear regression* e *multiple regression* in base alla quantità di variabili da relazionare: di numero pari a due nel primo tipo, di numero superiore a due nel secondo[111].

Illustrata la prima categoria *machine learning*, è utile passare alla seconda. Quest'ultima prende il nome di apprendimento automatico semi-supervisionato e si differenzia dalla prima declinazione poiché gli *input* forniti all'algoritmo consistono in una commistione di dati classificati e non[112]. Lo sfruttamento di una combinazione eterogenea di impulsi viene considerata la strategia migliore per elaborare un modello idoneo a classificare informazioni ed effettuare previsioni in maniera più precisa ed

[109] Nelle operazioni di classificazione, gli oggetti di natura simile vengono classificati in uno stesso gruppo. Per fornire un esempio del funzionamento della stessa: dato un gruppo di cento studenti, si richiede di raggrupparli in tre categorie in base alle loro altezze. Si procede dapprima con la misurazione dell'altezza di ogni studente e in seguito, alla luce dei risultati, si posiziona ognuno di essi in un dato gruppo. Così facendo per ogni singolo alunno, si insegnerà alla macchina come si formano i gruppi fino a quando la stessa sarà in grado di classificare correttamente qualsiasi nuovo studente in maniera autonoma. Conclusa questa fase di *training*, occorre testare il computer per verificare che abbia appreso la tecnica correttamente. In caso di risposta affermativa, lo stesso sarà idoneo ad essere mettere in produzione.

[110] Sul punto v. ROEPKE, *Go Beyond Binary Classification with Multi-Class and Multi-Label Models*, in Towards Data Science, 2022 *https://towardsdatascience.com/go-beyond-binary-classification-with-multi-class-and-multi-label-models-6ce91ca08264*

[111] In argomento v. TAM, *Simple and Multiple Linear Regression for Beginners*, 2020 *https://thomasttam.medium.com/simple-and-multiple-linear-regression-for-beginners-c852ffed6700*

[112] Sul punto v. SONI, *Machine Learning, i diversi modelli di apprendimento automatico*, in AI4buisness, 2019 *https://www.ai4business.it/intelligenza-artificiale/machine-learning/modelli-di-apprendimento-automatico/*

efficace rispetto a quanto si ottiene avvalendosi delle tecniche di *machine learning* supervisionato.

Il terzo sottoinsieme prende il nome di apprendimento non supervisionato poiché, a differenza dei precedenti, si basa sull'addestramento di un algoritmo attraverso informazioni che non subiscono né una classificazione né un'etichettatura[113]. Il metodo di *training* adottato consiste infatti nell'esporre la macchina a grandi volumi di dati non catalogati e consentire alla sessa di apprendere dalle informazioni ed agire di conseguenza senza il supporto di una linea guida ben precisa.

La quarta ed ultima declinazione di apprendimento automatico prende il nome di *reinforced machine learning* o apprendimento per rinforzo. La suddetta declinazione di apprendimento automatico si differenzia dalle tre categorie precedentemente illustrate in quanto l'algoritmo non viene affatto allenato attraverso la somministrazione di dati ed indicazioni precise. Lo scopo del *reinforcement learning* consiste, infatti, nel mettere la macchina nelle condizioni di risolvere problemi complessi attraverso l'interazione con l'ambiente circostante, così da mettere in pratica ciò che ha imparato senza il bisogno di alcun *input* o istruzione proveniente dell'essere umano[114].

La fase di *training* consiste, in concreto, nell'inserire l'algoritmo in un ambiente di simulazione, vale a dire un contesto nel quale il computer agisce senza ricevere alcuna informazione in anticipo su quale sia la migliore strategia da adottare nel caso concreto. Una volta operato in completa autonomia, il *tool* riceve un *feedback* che si sostanzia, alternativamente, in una ricompensa o in una penalità a seconda dell'efficacia dell'azione intrapresa. Questa tecnica basata sulla strategia *trial-and-error* consente al *software* di imparare a stimare le conseguenze

[113] Sul tema v. WOOD, *What is Unsupervised Learning?*, in *DeepAI, https://deepai.org/machine-learning-glossary-and-terms/unsupervised-learning*

[114] Cfr. KAELBLING, LITTMAN, MOORE, *Reiforcment learning: a survey, in Journal of Artificial Intelligence*, 1996, 237

di determinate azione e abilita lo stesso a sviluppare strategie a lungo termine per massimizzare le ricompense[115].

Gli ultimi sviluppi in tema di *machine learning* hanno condotto all'elaborazione di un'ultima sottocategoria, anche conosciuta come *Deep learning* o apprendimento profondo.[116] Già dalla denominazione è possibile intuirne la complessità nonché l'oscurità: gli algoritmi coinvolti, infatti, per via dell'alto numero di operazioni poste in essere nonché per la complessità delle stesse, non risultano perfettamente conoscibili neanche per i soggetti che li hanno programmati.[117] A ben vedere, quella dell'opacità rappresenta una caratteristica propria di tutti i *software* di intelligenza artificiale e la sua rilevanza varia in base al grado di indipendenza proprio dei diversi paradigmi tecnologici, raggiungendo la massima espressione nei *tools* che si avvalgono delle tecniche di *deep learning*. Quest'ultima costituisce uno dei principali *vulnus* delle tecnologie di IA in quanto, se non adeguatamente gestita e regolamentata, risulta idonea a generare violazioni delle normative in vigore e dei diritti fondamentali dell'uomo[118].

A seguito dell'analisi dei principali paradigmi di intelligenza artificiale, risulta chiaro come la loro capacità di analizzare la realtà complessità, la possibilità di passare in rassegna un insieme ampio e variegato di dati ed informazioni, la potenzialità di conseguire un obiettivo specifico predeterminato dall'uomo nonché la capacità di replicare le facoltà del ragionare, apprendere, decidere ed operare, tradizionalmente riconducibili alla sola intelligenza umana, rappresentano delle opportunità che andrebbero sfruttare altresì a supporto della *compliance* dell'ente, vale a dire nell'esecuzione degli adempimenti organizzativi che consentono alla

[115] Per un approfondimento sul punto v. KAELBLING, LITTMAN, MOORE, *Reiforcment learning*, cit., 238 ss.
[116] In tema v. SARKER, *Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions*, in *SN Computer Science*, 2021, 1 ss.
[117] Gli algoritmi di *deep learning* sono stati definiti *"Black.box"* poiché è possibile conoscere la soluzione fornita dagli stessi ma non anche l'insieme dei passaggi che hanno portato a quest'ultima, sul punto v. SARKER, *Deep Learning: A Comprehensive Overview*, cit., 1
[118] Il connotato dell'opacità e i rischi che ne derivano saranno oggetto di un approfondimento specifico nel capitolo terzo del presente lavoro di ricerca

persona giuridica di essere conforme alla normativa in vigore e di non incorrere nella verificazione di un reato al suo interno.

Per completare l'analisi relativa alle nuove tecnologie, appare ora opportuno offrire una panoramica dei principi, delle disposizioni normative in vigore nonché delle proposte volte a regolamentare i nuovi paradigmi digitali passati in rassegna.

3. Carta etica europea: i cinque principi per il corretto utilizzo dell'IA

A questo punto della trattazione risulta ormai assodato che la diffusione e lo sviluppo delle nuove tecnologie di intelligenza artificiale abbiano contribuito notevolmente al processo di trasformativo della società odierna. Si è in presenza di una vera e propria «rivoluzione tecnologica»[119] idonea ad impattare sullo svolgimento di numerose attività quotidiane che fino allo scorso ventennio appartenevano alla sola sfera di competenza dell'uomo.

Se le principali destinatarie del cambiamento in atto risultano essere le organizzazioni produttive in quanto, come dimostrato nei paragrafi precedenti, i processi decisionali interni alle stesse appaiono sempre più influenzati dalle risultanze dei processi algoritmici; anche il diritto e tutti i settori della giustizia, in tempistiche e modalità diverse, sono entrati a contatto con le nuove tecnologie[120] e ne stanno sperimentando le conseguenze.

Come affermato da autorevole dottrina, l'incontro tra il diritto ed i nuovi paradigmi tecnologici era inevitabile[121], quest'ultimo infatti è ontologicamente legato alle dinamiche sociali e, sin dall'inizio dei tempi, ancora la propria ragione d'esistere alla necessità di regolamentare le varie istanze sociali[122].

---

[119] Cfr., SEVERINO, *Intelligenza artificiale e diritto penale*, in RUFFOLO (a cura di), *Intelligenza artificiale: il diritto, i diritti, l'etica*, 2020, 531.

[120] Sul punto v. QUATTROCOLO, *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente discussione tra scienze penali e informatiche*, in *Leg. pen*., 2018, 2.

[121] In argomento v. UBERTIS, *Intelligenza artificiale*, cit., 76.

[122] Lo dimostra l'antico quanto celebre brocardo *Ubi societas, ibi ius*

Il compito del giurista ad ogni livello consiste proprio nel fornire soluzioni efficaci alle nuove sfide che emergono quotidianamente, nel caso di specie l'impiego dei recenti paradigmi tecnologici, operando un bilanciamento tra i benefici derivanti dall'utilizzo degli stessi e i rischi che ne conseguono, talvolta idonei a mettere a repentaglio i diritti fondamentali dell'uomo[123].

Ad oggi è assente una legislazione sia in ambito nazionale che comunitario volta a regolamentare la materia in maniera organica ed uniforme. Un tentativo di elaborare delle linee guida in merito al corretto utilizzo dell'IA indirizzate, in modo particolare, ai legislatori nazionali ed europei, proviene dal Consiglio d'Europa. Nel dicembre del 2018 è stata infatti pubblicata la Carta Europea per l'uso dell'intelligenza artificiale nei sistemi di giustizia penale e nei relativi ambienti[124], un documento stilato dalla Commissione europea per l'efficacia della giustizia (CEPEJ)[125] contenente i cinque principi fondamentali da rispettare nell'utilizzo degli algoritmi di intelligenza artificiale.

La Carta Etica Europea rappresenta un emblematico esempio di *soft law*[126] pensato per conseguire un duplice obiettivo, come ampliamente illustrato nell'introduzione al provvedimento.

Da un lato il Consiglio d'Europa si dimostra consapevole della crescente importanza dell'intelligenza artificiale nelle società moderne e dei benefici che possono derivare da un suo impiego nei sistemi giudiziari, giungendo alla conclusione che l'impiego di metodi computazionali a servizio della giustizia vada incoraggiato perché idoneo a migliorarne la qualità e l'efficienza.

Dall'altro, il Consiglio è a conoscenza delle problematiche connesse all'impiego dell'IA e delle possibili violazioni dei diritti umani, come in

[123] Sul tema v. SEVERINO, *Intelligenza artificiale*, cit., 531.
[124] Il testo integrale della carta è disponibile sul sito ufficiale del Consiglio d'Europa: *https://publicsearch.coe.int/#k=#f=%5B%5D*
[125] La Commissione europea per l'efficacia della giustizia (CEPEJ) è stata istituita nel 2002 per iniziativa del Comitato dei Ministri del Consiglio d'Europa con lo scopo di monitorare e misurare la qualità dei sistemi giudiziari dei Paesi membri. Per maggiori informazioni a riguardo consultare il situ ufficiale: *https://www.coe.int/en/web/cepej/home*
[126] In argomento v. QUATTROCOLO, *Intelligenza artificiale e giustizia*, cit., 3.

parte dimostrato dallo studio intitolato *Algorithms and Human rights*[127], pubblicato da parte della stessa organizzazione internazionale nei mesi precedenti all'emanazione della Carta. La sfida consiste pertanto nell'incentivare l'utilizzo dei nuovi tools, purché sia responsabile e *compliant* ai diritti fondamentali della persona[128].

I destinatari della Carta risultano essere sia soggetti pubblici che privati coinvolti a vario titolo nella realizzazione e nell'impiego di strumenti di intelligenza artificiale. Il documento è indirizzato in modo particolare ai legislatori, i quali vengono invitati ad elaborare una cornice normativa volta a regolamentare la programmazione e l'utilizzo dell'intelligenza artificiale nel rispetto dei cinque principi delineati dalla Carta Etica Europea, di cui è utile illustrarne il contenuto. [129]

Il primo principio mira ad assicurare il rispetto dei diritti fondamentali[130]. Nella nota esplicativa che accompagna la Carta vengono menzionati due documenti principali[131] i quali contemplano una serie di diritti e garanzia da tenere in considerazione nella realizzazione[132] e nell'utilizzo delle tecnologie di intelligenza artificiale, qualunque sia il loro impiego specifico[133]. La questione che si pone attiene ai significati nonché ai risvolti pratici degli stessi, il più delle volte, patrimonio conoscitivo dei soli studiosi del diritto. È per tale motivo che si auspica una solida collaborazione tra aree del sapere, nel caso di specie tra giuristi ed esperti di tecnologie, nonostante l'assenza di spazi ad hoc e di un vero e proprio linguaggio comune[134].

---

[127] Lo studio è stato condotto nel 2017 ed i risultati dello stesso sono reperibili sul sito ufficiale del Consiglio d'Europa: *https://www.coe.int/web/artificial-intelligence/home*

[128] Sul punto v. BARBARO, *Cepej, adottata la prima Carta etica europea sull'uso dell'intelligenza artificiale (AI) nei sistemi giudiziari*, in *Questione giustizia*, 2018.

[129] Cfr. QUATTROCOLO, *Intelligenza artificiale e giustizia*, cit., 3

[130] V. Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi, p. 8

[131] Si fa riferimento alla Convenzione europea dei diritti dell'uomo e alla Convenzione per la protezione dei dati personali

[132] La nota esplicativa che accompagna la Carta utilizza la locuzione *human-rights-by-design*

[133] Si richiede, in particolare, la *compliance* con il diritto ad un equo processo, il diritto al contraddittorio in tutte le sue declinazioni, l'imparzialità e terzietà dei giudici, il dritto alla privacy, il principio di legalità e così via, tutte garanzie da tempo cristallizzate nelle costituzioni degli Stati democratici, sul punto v. QUATTROCOLO, *Intelligenza artificiale e giustizia*, cit., 4.

[134] In argomento v. QUATTROCOLO, *Intelligenza artificiale e giustizia*, cit., 5.

Il secondo principio contemplato dalla Carta è quello di non discriminazione[135]. I sistemi computazionali che si occupano di raggruppare e analizzare grandi quantità di dati, il più delle volte personali[136], tendono ad evidenziare la presenza di discriminazioni o ad accentuarne l'esistenza, come precisato nell'appendice esplicativa alla Carta. Le tecnologie di intelligenza artificiale sono infatti esposte al rischio di c.d. *implicit bias*[137], vale a dire errori intrinseci che il più delle volte derivano dalla mancata neutralità dell'*input* fornito. Ne consegue un *output* geneticamente falsato perché influenzato dal pregiudizio, il quale contribuirà a generare differenziazioni infondate tra singoli individui o gruppi di persone.

La Commissione, facendo leva sul secondo principio in esame, consiglia di esercitare una concreta attività di vigilanza sia nella fase di creazione che in quella di utilizzo degli algoritmi di intelligenza artificiale, ponendo particolare attenzione ai casi in cui vengono coinvolti i dati personali sensibili[138]. In presenza di questi ultimi, infatti, si impone di prevedere misure correttive al fine di limitare o, se possibile, neutralizzare i suddetti rischi di discriminazione. Per conseguire al meglio gli obiettivi prefissati, si auspica l'istaurazione di uno stretto rapporto di collaborazione tra esperti di intelligenza artificiale, studiosi delle interazioni sociali e giuristi[139].

Il terzo principio[140] presente nella Carta mira a garantire la qualità e la sicurezza dei paradigmi di IA impiegati nell'analisi di dati e decisioni giudiziarie. La Commissione europea per l'efficacia della giustizia ha

[135] V. Carta etica europea sull'utilizzo dell'intelligenza artificiale, cit., p. 9

[136] Per dato personale si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile. La seguente definizione è contenuta nell'art. 4 del Regolamento generale sulla protezione dei dati (GDPR).

[137] Per approfondimenti sul punto v. MILANO, *Turning a light on our implicit biases,* in *Harvard Gazzette*, 2020. Il contributo è disponibile al seguente *link*: *https://news.harvard.edu/gazette/story/2020/12/taking-a-hard-look-at-our-implicit-biases/*

[138] La definizione di dati sensibili è contenuta nell'art 9 GDPR, questi ultimi sono i dati personali che riguardano la sfera più intima del soggetto. Nella categoria rientrano: l'origine razziale o etnica, le condizioni socioeconomiche, le opinioni politiche, la fede religiosa o filosofica, l'appartenenza a un sindacato, i dati genetici, i dati biometrici, i dati sanitari e così via.

[139] Sul punto v. QUATTROCOLO, *Intelligenza artificiale e giustizia*, cit., 6.

[140] V. Carta etica europea sull'utilizzo dell'intelligenza artificiale, cit., p. 10

elaborato tre raccomandazioni principali, funzionali al rispetto del suddetto principio.

In primo luogo, si richiede l'utilizzo di fonti certificate e dati intangibili. Risulta, infatti, di fondamentale importanza verificare l'attendibilità della sorgente dalla quale proviene l'informazione nonché l'integrità della stessa. L'intero processo deve essere pertanto tracciabile così da garantire che non abbia avuto luogo alcuna modifica idonea ad alterare il contenuto o il significato della decisione assunta.

In secondo luogo, la Commissione raccomanda che gli algoritmi su cui si basa la decisione giudiziaria vengano custoditi in un ambiente tecnologico sicuro e impenetrabile, nell'ottica di evitare modificazioni e alterazioni improprie degli stessi.

In ultimo, si auspica l'adozione di un approccio multidisciplinare nella creazione di modelli computazionali, così da assicurarne la completezza e la sicurezza: la Commissione consiglia, in particolare, di costituire squadre di progetto miste che vedano la presenza sia di esperti di informatica capaci di progettare modelli di apprendimento automatico che di professionisti del sistema giustizia come giudici, pubblici ministeri, avvocati, e ricercatori nel campo del diritto e delle scienze sociali[141].

Il quarto principio[142] delineato dalla Carta ha ad oggetto la trasparenza, l'imparzialità e l'equità: tre requisiti fondamentali che devono connotare tutti gli algoritmi di intelligenza artificiale. A garanzia degli stessi, la Commissione suggerisce sia di rendere accessibili e facilmente comprensibili le metodologie di trattamento dei dati che di autorizzare verifiche periodiche da parte di professionisti esterni. Si auspica inoltre il raggiungimento di un equilibrio[143] tra la proprietà intellettuale di alcune

[141] In argomento v. QUATTROCOLO, *Intelligenza artificiale e giustizia*, cit., 6.
[142] V. Carta etica europea sull'utilizzo dell'intelligenza artificiale, cit., p. 11
[143] A tale riguardo è interessante la soluzione delineata a p. 38 dello studio "*Algorithms and Human rights*" pubblicato dal Consiglio d'Europa nel 2017: piuttosto che imporre alle imprese la pubblicazione integrale del testo di un algoritmo o del codice di un *software*, preso atto del loro interesse a mantenerli privati, sarebbe preferibile richiedere che siano divulgate al pubblico le informazioni fondamentali quali, ad esempio, le variabili utilizzate, gli obiettivi a cui è finalizzata l'ottimizzazione degli algoritmi, i dati di apprendimento, la quantità e il tipo di dati trattati dall'algoritmo.

metodologie di trattamento, prevista e garantita dal terzo principio della Carta, e l'esigenza di trasparenza, imparzialità, equità ed integrità intellettuale nell'utilizzo di strumenti che possano determinare conseguenze in ambito giuridico o, più in generale, idonee ad incidere significativamente sulla vita delle persone.

La soluzione prospettata dalla Carta non si presta a dubbi interpretativi: si raccomanda, infatti, una completa trasparenza in merito agli elementi tecnici che connotano un *tool*, implementata da una relazione volta ad illustrare il funzionamento del processo computazionale in un linguaggio chiaro ed accessibile a tutti, attestando in questo modo la prevalenza del quarto principio sopra illustrato[144].

La Commissione non ignora che la comprensione del modello rimane, nella maggior parte dei casi, una questione limitata ai soli esperti, con esclusione degli effettivi destinatari della "decisione automatizzata". Questa circostanza va a minare i principi fondamentali della pubblicità del processo decisionale e della valutazione della prova, garantiti nella maggior parte degli ordinamenti democratici.

In aggiunta, la "trasparenza algoritmica", alla luce dell'elevato tecnicismo che caratterizza i meccanismi di funzionamento delle nuove tecnologie, non è sufficiente, da sola, a consentire al giudice e ai destinatari della sentenza di comprendere a pieno il procedimento logico che ha condotto a generare una data prova digitale[145]. Per ovviare a quest'inconveniente, la Commissione suggerisce di coinvolgere autorità esterne ed indipendenti con lo scopo di verificare periodicamente l'attendibilità degli algoritmi utilizzati nei servizi di giustizia.

Quinto ed ultimo principio[146] enunciato dalla Carta Etica Europea attiene al controllo da parte dell'utilizzatore. La Commissione è convinta che l'impiego dei nuovi paradigmi tecnologici debba potenziare e non

[144] Sul tema v. QUATTROCOLO, *Intelligenza artificiale e giustizia*, cit., 8.
[145] Nell'ordinamento italiano, secondo quanto sancito dall'art. 111 co. 6 Cost., è nella motivazione della sentenza che si deve dare conto pubblicamente del percorso logico e argomentativo che ha condotto all'assunzione di una prova e, più in generale, alla decisione incardinata nella stessa. Per un approfondimento sul punto v. TONINI, CONTI, *Manuale di procedura penale*, Milano, 2021, 787.
[146] V. Carta etica europea sull'utilizzo dell'intelligenza artificiale, cit., p. 12

limitare l'autonomia e la libertà di scelta del soggetto che se ne avvale. Se tale conclusione viene declinata ai professionisti della giustizia quali fruitori delle nuove tecnologie, ne consegue sia il loro diritto a rivedere le decisioni giudiziarie nonché i dati utilizzati per produrre un dato risultato, che il diritto di non essere necessariamente vincolati da quest'ultimo in caso di mutamento delle circostanze concrete.

Se, invece, per beneficiario dell'intelligenza artificiale si fa riferimento al cittadino sottoposto a processo, ne deriva la sua legittima pretesa di essere informato in un linguaggio chiaro e comprensibile circa le diverse soluzioni prospettate dall'algoritmo di IA, di avere la possibilità di accedere ad un tribunale, di vedersi sempre garantita un'assistenza legale, nonché di ricevere comunicazione circa gli esiti dei procedimenti conclusi in precedenza con una decisione basata, in tutto o in parte, sull'intelligenza artificiale, con conseguente diritto di opporvisi e far giudicare il proprio caso da un giudice in un tribunale[147][148].

In ultimo, per una completa ed effettiva applicazione del quinto principio contenuto nella Carta, la Commissione suggerisce l'istituzione di programmi di alfabetizzazione informatica quando i destinatari degli output prodotti dai tools risultano essere soggetti profani[149].

Una volta illustrati i cinque principi da rispettare sia nella programmazione che nell'utilizzo dell'intelligenza artificiale, la Commissione prospetta l'esigenza che gli stessi siano sottoposti a regolare applicazione, monitoraggio nonché valutazione da parte di esperti sia pubblici che privati, così da garantire un continuo miglioramento delle prassi.

Per concludere, in caso di violazione dei principi contenuti nella Carta si ritiene opportuno che venga pubblicata una relazione da parte dei professionisti che hanno rilevato l'irregolarità in modo da illustrarne i

[147] In virtù di quanto stabilito dall'art 6 CEDU
[148] Sul punto v. QUATTROCOLO, *Intelligenza artificiale e giustizia*, cit., 9 s.
[149] V. Carta etica europea sull'utilizzo dell'intelligenza artificiale, cit., p. 12

motivi e accompagnare la stessa con un piano di azione volto a suggerire le misure necessarie da adottare[150].

Merita di essere segnalato il mandato conferito dal Consiglio d'Europa a un'*equipe* di esperti che si sostanzia nell'adozione di un «*certification mechanism*»[151]: un procedimento volto ad attestare la *compliance* degli algoritmi di intelligenza artificiali utilizzati nei settori della giustizia ai cinque principi contenuti nella Carta Etica Europea, tutt'ora in via di sperimentazione[152].

In aggiunta, il Consiglio dei ministri del Consiglio d'Europa ha istituito l'*Ad Hoc Committee on Artificial Intelligence*[153], un comitato costituito da rappresentati dei 47 Stati Membri dell'Organizzazione Internazionale con il compito di elaborare una cornice normativa idonea a regolamentare la programmazione, l'impiego e l'evoluzione delle tecnologie di intelligenza artificiale, basato sulle norme del Consiglio d'Europa in materia di diritti umani, democrazia e Stato di diritto.

4. Proposta europea per la regolamentazione dei sistemi di IA

Nell'ultimo quinquennio sono molteplici le comunicazioni, i programmi politici ed i provvedimenti di *soft law*[154] che hanno testimoniato l'esigenza di emanare un testo legislativo a livello comunitario volto a regolamentare la programmazione e il funzionamento delle nuove tecnologie di IA.

La proposta di regolamento europeo[155] avanzata dal Parlamento europeo e dal Consiglio rappresenta la prima risposta concreta alla suddetta

[150] V. Carta etica europea, cit., 4

[151] Per approfondimenti sul punto consultare il sito ufficiale del Consiglio d'Europa al seguente *link*: *https://publicsearch.coe.int/#k=certification%20mechanism#f=%5B%5D#s=51*

[152] In argomento v. SEVERINO, *Intelligenza artificiale*, cit., 544.

[153] *L'Ad Hoc Committee on Artificial Intelligence* è stato istituito in data 11 settembre 2019, per un approfondimento sul punto è possibile consultare il sito ufficiale dell'Unione europea: *https://www.coe.int/en/web/artificial-intelligence/cahai-1*

[154] Si fa riferimento, in modo particolare, al Libro bianco sull'intelligenza artificiale e alla Carta Etica europea, cfr. Proposta europea per la regolamentazione dei sistemi di IA, 1 s.

[155] La Proposta europea per la regolamentazione dei sistemi di IA è stata pubblicata in data 21 aprile 2021 a seguito delle consultazioni dei principali portatori di interessi, consultabili : *https://ec.europa.eu/digital-single-market/en/news/white-paper-artificial-intelligence-public-consultation-towards-european-approach-excellence*

impellente esigenza di normazione. Quest'ultima è, infatti, orientata a stabilire regole armonizzate in materia di intelligenza artificiale e a modificare alcuni atti legislativi dell'Unione[156]; fa parte, inoltre, di un compendio di misure più ampio, tutte indirizzate ad affrontare le criticità connesse alle nuove tecnologie progettate negli ultimi decenni. [157]

La relazione che accompagna la proposta di regolamento europeo chiarisce ampliamente quali siano i motivi che giustificano l'adozione del provvedimento legislativo e gli obiettivi che si intendono perseguire con lo stesso.

Quanto alle motivazioni, esse sono duplici. Da un lato vi è una maturata consapevolezza circa le potenzialità connesse all'impiego dell'intelligenza artificiale[158], che si dimostra in grado di offrire un contributo notevole per il raggiungimento di risultati di segno positivo a livello sociale e risulta capace di migliorare le economie europee, rendendo più competitive le imprese del tessuto economico comunitario[159], in modo particolare quelle che operano nei settori «ad alto impatto»[160]. Dall'altro, si fa riferimento ai nuovi rischi o conseguenze negative a scapito delle persone fisiche e della società che derivano dall'utilizzo delle nuove tecnologie[161], le quali contribuiscono a creare un ecosistema di sfiducia generale nei confronti della rivoluzione tecnologica che si auspica.

L'intento dell'Unione europea consiste, pertanto, sia nel preservare e potenziare la *leadership* tecnologica dell'UE che nell'operare un bilanciamento tra potenzialità da un lato e rischi dall'altro, così da assicurare

[156] Come precisato nel titolo della stessa

[157] Un elenco delle stesse è contento nella Relazione che accompagna la Proposta di regolamento europeo, 5.

[158] Definita nella Relazione di accompagnamento come una famiglia di tecnologie in rapida evoluzione, in grado di apportare una vasta gamma di benefici economici e sociali in tutto lo spettro delle attività, cfr., Proposta europea per la regolamentazione dei sistemi di IA, 1 s.

[159] Le nuove tecnologie contribuiscono al miglioramento nel fare previsioni, all'ottimizzazione delle operazioni e alla più efficiente assegnazione delle risorse e alla personalizzazione dell'erogazione di servizi, sul punto v. Proposta europea per la regolamentazione dei sistemi di IA, 20.

[160] Esempi di settori ad alto impatto sono quelli che operano in materia di cambiamenti climatici, ambiente, sanità, finanza, mobilità, affari interni, agricoltura, come esplicitato dalla Relazione alla proposta.

[161] L'impiego dell'intelligenza artificiale può compromettere il rispetto dei diritti umani, primo fra tutti il diritto alla *privacy*.

che i cittadini europei possano beneficiare delle nuove tecnologie sviluppate in conformità ai valori, ai diritti fondamentali e ai principi dell'Unione. [162]

Gli obiettivi specifici[163] che la proposta di regolamento mira a conseguire vengono suggeriti, come da prassi, dalla Commissione e si focalizzano su quattro punti principali. In *primis*, risulta necessario assicurare che i sistemi di Intelligenza artificiale immessi nel mercato dell'Unione siano sicuri e rispettosi della normativa vigente in materia di diritti fondamentali e aderenti ai valori comuni. In secondo luogo, occorre garantire la certezza del diritto, presupposto fondamentale per favorire l'intensificazione della ricerca scientifica e per facilitare gli investimenti in materia.

Il terzo obiettivo prioritario è rappresentato dal miglioramento della *governance* e dall'applicazione effettiva delle norme esistenti in materia di dritti fondamentale e requisiti di sicurezza ai sistemi di IA.

In ultimo, la Commissione individua nello sviluppo agevole di un mercato unico in materia di tecnologie di intelligenza artificiale il quarto risultato da conseguire con il contributo normativo in esame[164]. Quest'ultimo, a ben vedere, rappresenta lo scopo più ambito, tanto che, quale base giuridica della Proposta di regolamento, si indica l'art. 114 TFUE[165].

Il Parlamento europeo e il Consiglio, come precisato nella relazione accompagnatrice, concordano nel conseguire gli obiettivi sopra elencati avvalendosi di un approccio normativo orizzontale nonché orientato alla sussidiarietà e proporzionalità[166]. La proposta di regolamento, pertanto, si limita a stabilire i requisiti minimi necessari a scongiurare i rischi connessi

[162] Sul punto v. LAVORGNA, SUFFIA, *La nuova proposta europea per regolamentare i Sistemi di Intelligenza Artificiale e la sua rilevanza nell'ambito della giustizia penale*, in Riv. Trim., 2021, 89, 92.
[163] V. Proposta europea per la regolamentazione dei sistemi di IA, 3.
[164] Cfr., Proposta europea per la regolamentazione dei sistemi di IA, 6.
[165] L'articolo 114 TFUE abilita le istituzioni dell'Unione europea ad emanare misure orientate alla creazione e al funzionamento del mercato unico interno. V. Proposta europea per la regolamentazione dei sistemi di IA, 6 s.
[166] L'intento è quello di non limitare lo sviluppo tecnologico in materia e di non rendere eccessivamente oneroso il procedimento di immissione delle nuove tecnologie sul mercato. V. Proposta europea per la regolamentazione dei sistemi di IA, 6; In argomento v. LAVORGNA, SUFFIA, *La nuova proposta europea*, cit., 92.

all'utilizzo delle nuove tecnologie e predilige l'adozione di strumenti flessibili, idonei cioè ad adattarsi alla rapida evoluzione delle tecnologie e all'emersione di nuove problematiche.

Il connotato dell'orizzontalità[167] implica un'assoluta coerenza delle nuove regole delineate con la Proposta sia con la normativa vigente nei settori in cui le tecnologie di intelligenza artificiale sono impiegate, che con il diritto europeo[168].

Il requisito della sussidiarietà[169] si basa sulla consapevolezza che la presenza di un mosaico di regole nazionali frammentarie sia scarsamente proficua e addirittura di ostacolo alla prevenzione nonché gestione dei rischi connessi all'impiego dei sistemi di IA. La natura stessa delle tecnologie di intelligenza artificiale dimostra che gli obiettivi fissati dalla proposta possano essere conseguiti in maniera più ottimale attraverso l'elaborazione di un approccio unico a livello comunitario, orientato a stabilire regole paritarie e generalmente applicabili all'interno del mercato unico europeo.

Quanto alla caratteristica della proporzionalità[170], quest'ultima implica l'adozione di un approccio che si traduca in un'ingerenza minima necessaria della legislazione europea sui sistemi giuridici settoriali già in vigore. L'intero impianto normativo delineato dalla proposta è infatti improntato alla gestione del rischio[171] e l'approccio proposto varia a seconda di quanto le diverse declinazioni di IA siano propense a generare violazioni della legislazione europea e dei diritti fondamentali dell'uomo, sulla base di una distinzione tra le stesse effettuata a monte[172].

---

[167] V. Proposta europea, cit., 4.

[168] Particolare menzione viene fatta nei confronti della Carta dei diritti fondamentali dell'unione Europea, del GDPR, della normativa a tutela dei consumatori, della parità di genere e della non discriminazione, tutti provvedimenti che la proposta di regolamento si limita ad integrare senza sostituirsi ad essi.

[169] Sul punto v. Proposta europea, cit., 7.

[170] Cfr. Proposta europea, cit., 7.

[171] Sul punto v. MINELLI, *La responsabilità "penale" tra persona fisica e corporation alla luce della Proposta di Regolamento sull'Intelligenza Artificiale*, in *Riv. Trim. Dir. Cont. Pen.*, 2/2022, 52.

[172] Nel titolo II della Proposta di regolamento vengono delineate tre diverse categorie di IA alle quali è dedicato un approccio *ad hoc*: quelle che comportano un rischio inaccettabile, quelle che implicano un rischio alto ed infine quelle connesse ad un rischio basso o minimo. Sul punto v. Proposta europea, cit., 14.

Una scelta categorica investe talune pratiche di IA, queste ultime sono vietate perché risultano particolarmente dannose e in contrasto con i valori dell'unione. Una strategia diversa, utile alla gestione del rischio, viene invece messa in campo per regolare i c.d. «sistemi di IA ad alto rischio»[173]: gli stessi dovranno integrare dei requisiti obbligatori ed essere sottoposti a procedure di valutazione della conformità in un momento precedente alla loro immissione nel mercato. Vincoli meno incisivi che si concretizzano in obblighi minimi di trasparenza sono, infine, previsti in relazione a sistemi specifici di IA, per natura più sicuri e trasparenti.

La scelta del regolamento[174] come atto giuridico più idoneo a dettare regole unitarie in materia di intelligenza artificiale si giustifica alla luce della sua diretta e uniforme applicabilità in tutti gli Stati membri, idonea ad evitare la frammentarietà delle normative e la diversità di approccio alla materia tra nazioni. Il regolamento mira, pertanto, alla costituzione di un sistema comune europeo fondato sulla cooperazione tra stati membri, che si avvale di strutture già esistenti ed è garantito dalla presenza di un comitato europeo per l'intelligenza artificiale.

A stemperare la tendenziale rigidità del suddetto strumento legislativo che, a differenza della direttiva, non si limita a fissare gli obiettivi da perseguire ma fissa altresì regole ben precise per la loro attuazione[175], vengono inseriti spazi di sperimentazione normativa volti a favorire lo sviluppo dell'innovazione e ad alleggerire gli oneri normativi, in alcuni casi particolarmente gravosi per le PMI e le *startup*.

Entrando nel merito della proposta di regolamento, è utile fornire una panoramica dei dodici titoli che la compongono. Il titolo uno ricomprende gli articoli 1, 2 e 3 del decreto e si occupa, in *primis*, di delineare l'oggetto del regolamento[176]. Quest'ultimo coincide con

[173] Vengono definiti ad alto rischio perché sono potenzialmente idonei ledere il diritto alla salute, alla sicurezza e ulteriori diritti fondamentali delle persone. In argomento v. LAVORGNA, SUFFIA, *La nuova proposta europea*, cit., 93
[174] Cfr., Proposta europea, cit., 7 s.
[175] Per un approfondimento sul punto v. STROZZI, MASTROIANNI, *Diritto dell'unione europea parte istituzionale*, Roma, 2020, 290 ss.
[176] V. art 1 Proposta di regolamento cit.

l'emanazione di regole armonizzate volte a normare l'immissione sul mercato, la messa in servizio e l'utilizzo delle tecnologie di intelligenza artificiale. Oggetto del decreto sono altresì i divieti di alcune pratiche di intelligenza artificiale, i requisiti specifici da integrare in relazione ai sistemi di IA ad alto rischio nonché gli obblighi da rispettare per chi opera in tali sistemi. In aggiunta, si guarda all'emanazione di regole a garanzia della trasparenza di quelle declinazioni di IA che per loro natura interagiscono con le persone ed infine, vengono ricomprese le disposizioni utili a monitorare e vigilare il mercato delle nuove tecnologie.

L'ambito di applicazione del regolamento è definito dall'articolo 2 dello stesso: si fa riferimento ai fornitori di servizi di intelligenza artificiale, agli utenti situati nel territorio dell'Unione Europea e ai fornitori nonché agli utenti situati in un Paese terzo ma che si occupano di algoritmi di IA i cui *output* vengono utilizzati nell' Unione Europea[177].

L'articolo 3 è orientato a chiarire il significato dei termini tecnici e scientifici utilizzati nel testo, compendia pertanto l'insieme delle definizioni dei termini e delle locuzioni principali: si esplicita, ad esempio, il significato dei sostantivi quali intelligenza artificiale, fornitore, utente, operatore e così via.

Il titolo 1 è altresì accompagnato dall'allegato 1[178] che compendia un elenco di approcci e tecniche idonee allo sviluppo dell'intelligenza artificiale indirizzato alla Commissione europea, affinché provveda alle dovute modifiche in presenza di nuove scoperte tecnologiche acquisite.

Procedendo nell'analisi sistematica del provvedimento in esame, il titolo 2 si occupa di elencare le pratiche di intelligenza artificiale da vietare perché ontologicamente lesive dei diritti fondamentali dell'uomo come, fornire un esempio concreto, l'insieme delle tecnologie idonee a provocare un danno fisico o psicologo ad una persona [179].

[177] Sul punto v. MINELLI, *La responsabilità "penale" tra persona fisica e corporation*, cit. 52.
[178] Il testo integrale dell'allegato I è disponibile sul sito ufficiale dell'Unione europea *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52021PC0206&from=IT*
[179] V. art. 3 della Proposta di regolamento

La definizione dei sistemi ad alto rischio e dell'insieme di regole che riguardano questi ultimi è demandata al titolo terzo della proposta di regolamento, suddiviso a sua volta in cinque capi. Il primo tra questi si occupa di classificare le tecnologie di IA ad alto rischio[180], il secondo ne elenca i requisiti, il terzo fissa gli obblighi in capo ai fornitori e agli utenti che si avvalgono di tali sistemi, il quarto si occupa dell'autorità di notifica e degli organismi notificati ed il quinto detta le norme applicabili ai sistemi ad alto rischio nonché definisce i procedimenti di valutazione di conformità, i certificati richiesti ed il processo di registrazione.

Segue il titolo quarto volto a disciplinare i particolari sistemi di intelligenza artificiale che comportano rischi specifici di manipolazione[181], in relazione ai quali vengono previsti obblighi di trasparenza da rispettare.

Il titolo quinto detta, invece, un elenco di misure a sostegno dell'innovazione. Con lo stesso si incoraggiano gli Stati membri sia a creare forme di sperimentazione normativa da sottoporre ad un piano di prova concordato che ad alleggerire gli oneri normativi i capo alle PMI e alle *startup*.

Sono i titoli sesto e settimo ad occuparsi di *governance*. Si prevede infatti l'istituzione sia di un Comitato europeo per l'intelligenza artificiale[182] che di una o più autorità nazionali competenti in materia. I titoli in questione contemplano altresì la possibilità di costituire una banca dati a livello comunitario volta a facilitare il lavoro di controllo da parte della Commissione e delle autorità nazionali competenti. Al titolo ottavo è demandata la fissazione delle relative norme di attuazione.

La Proposta prosegue con il titolo nono, orientato a delineare un quadro normativo che consenta ai fornitori di sistemi di IA non ad alto rischio di stabilire in maniera autonoma i diversi codici di condotta: quel

[180] Vengono individuate due categorie principali di sistemi di IA ad alto rischio: i sistemi destinati ad essere utilizzati come componenti di sicurezza di prodotti ed i sistemi di IA indipendenti che influenzano la sfera dei diritti fondamentali esplicitamente elencati nell'allegato III alla Proposta di regolamento

[181] Si fa riferimento i primis ai sistemi di IA che interagiscono con gli esseri umani, in secondo luogo a quelli utilizzati per rilevare emozioni o stabilire un'associazione con categorie (sociali) sulla base di dati biometrici, in ultimo a quelli che generano o manipolano contenuti.

[182] Quest'ultimo deve essere composto dai membri di ciascuno Stato UE.

che si mira a garantire è un approccio focalizzato sulle peculiarità degli stessi.

A chiusura del testo legislativo in esame ci sono gli ultimi tre titoli, i quali contengono le disposizioni finali. Il titolo decimo, nello specifico, evidenzia l'obbligo generale di rispettare la riservatezza dei dati e stabilisce le regole per lo scambio delle informazioni ottenute durante l'attuazione del regolamento. Il titolo undicesimo fissa le regole per esercitare la delega e le competenze di esecuzione. Infine, il titolo dodicesimo contiene l'obbligo per la Commissione di valutare periodicamente la necessità aggiornare il testo normativo e suggerisce la predisposizione, a scadenze concordate, di relazioni che attestino il livello di *compliance* del testo ed eventuali proposte di emendamento dello stesso. Questo titolo conclusivo fissa, inoltre, un periodo transitorio differenziato in merito alla data di applicabilità del regolamento, così da garantire e agevolare la corretta attuazione del testo da parte di tutti gli interessati.

5. *Blockchain*: definizione, caratteristiche e funzionamento

Annoverabile tra le tecnologie ideate negli anni duemila e meritevole di un approfondimento specifico in virtù delle sue potenzialità intrinseche è la *Blockchain.* Quest'ultima fu teorizzata per la prima volta [183] nel saggio[184] che ha introdotto il *Bitcoin*, la prima criptovaluta pensata per i pagamenti elettronici *machine-to-machine* che per il suo funzionamento si avvale della tecnologia a registro distribuito[185].

L'impiego della tecnologia di blockchain a supporto della moneta virtuale garantisce la possibilità di superare il problema del *double spending money*[186], rendendo il *bitcoin* totalmente indipendente da ogni istituto

[183] Da parte di *Satoshi Nakamoto*, pseudonimo dell'inventore del *Bitcoin*

[184] NAKAMOTO, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2009. *https://nakamotoinstitute.org/bitcoin/*

[185] Le transazioni di *bitcoin* sono elaborate in maniera completamente decentralizzata e il loro svolgimento è garantito ma un meccanismo di consenso probabilistico chiamato PoW, sul punto v. DE ANGELIS, ZANFINO, ANIELLO, LOMBARDI, SASSONE, *Evaluating Blockchain Systems: A Comprehensive Study of Security and Dependability Attributes*, Roma, 2022, 20.

[186] Locuzione che indica il rischio di spendere due volte il medesimo importo di denaro

finanziario o autorità centrale garante, concepiti come fonti di costi, sprechi e lentezza nelle operazioni[187].

Prima di fornire una panoramica delle potenzialità connesse all'impiego di tale nuova tecnologia in molteplici ambiti della società, è utile definirla, chiarire quali siano le azioni esercitabili nel sistema ed evidenziarne le caratteristiche tecniche principali.

La *blockchain* appartiene alla più ampia categoria di tecnologie di *Distributed Ledger Technology* o DLT[188], vale a dire sistemi progettati mediante l'utilizzo di blocchi di dati concatenati gli uni agli altri attraverso soluzioni criptografiche[189], definiti nel 2018 dal legislatore italiano come «tecnologie e 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» [190].

In concreto la *blockchain*, letteralmente catena di blocchi, consiste in un registro distribuito e decentralizzato che sfrutta la crittografia asimmetrica per la protezione e l'autenticazione delle transazioni iscritte e conservate in blocchi collegati tra loro cronologicamente[191].

Le azioni esercitabili nel registro distribuito sono principalmente tre, quella di *read*, che implica l'accesso ai dati contenuti nel sistema, quella di

---

[187] In argomento v. GAMBINO, BOMPREZZI, *Blockchain e protezione dei dati personali*, in *Dir. Inf*, 2019, 624

[188] Le DLT sono "tecnologie in cui tutti i nodi di una rete possiedono la medesima copia in un database che può essere letto e modificato in modo indipendente dai singoli nodi. Le modifiche al registro vengono regolate tramite algoritmi di consenso che permettono di raggiungere il consenso tra le varie versioni del registro, nonostante esse vengano aggiornate in maniera indipendente dai partecipanti della rete", questa la definizione contenuta nel glossario elaborato da Osservatori.net a cura del Politecnico di Milano
https://blog.osservatori.net/it_it/distributed-ledger-technology-significato

[189] Si rimanda alla definizione 3.6, in *Blockchain and distributed ledger technologies — Terminology* (ISO/DIS 22739), aggiornato al 21 dicembre 2019

[190] La definizione riportata è contenuta nell'art 8 ter co.1 del d.l. 135/2018 convertito nella l. n. 12/2019

[191] In argomento v. CAPACCIOLI, *DLT e Blockchain*, in ZICCARDI, PERRI (a cura di), *Tecnologia e diritto*, Vol II, Milano, 2019, 372 ss; ACCINNI, *L'utilizzo criminogeno della blockchain: gli smart contract*, in *Sist. pen*., 2022, 133; GHIANI, *Blockchain: linee guida*, 2022, Torino, 13.

write, che abilita ad effettuare transazioni ed infine quella di *commit* che garantisce la possibilità di intervenire in maniera incisiva nel registro, aggiornandolo attraverso l'aggiunta di un nuovo blocco.

In relazione all'azione di *read*, è possibile distinguere tra tecnologia di *blockchain* pubblica, dove non sussiste alcuna restrizione nell'accesso alle informazioni contenute nel registro, e *blockchain* privata, all'interno della quale solo una cerchia predeterminata di soggetti è abilitata a leggere i dati del sistema.

Un'ulteriore distinzione è operata tra *blockchain permissionless* e *blockchain permissioned* poiché nella prima sottocategoria chiunque ha la possibilità di porre in essere azioni di *write* e *commit* mentre nella seconda tipologia queste ultime solo riservate ad un numero limitato di utenti[192].

Quanto alle caratteristiche proprie della tecnologia di *blockchain*, ne sono state individuate sei principali[193], che rappresentato tanto punti di forza quanto elementi generatori di rischi da prevedere e gestire.

La prima caratteristica fondamentale della tecnologia in esame è ravvisabile nella disintermediazione. Quest'ultima implica che le transazioni nelle piattaforme avvengano senza il contributo di soggetti terzi intermediari nonché in totale assenza di un'autorità centrale incaricata di certificare e garantire la veridicità delle stesse. Viene a mancare pertanto il rapporto di c.d. *«client-server»* proprio dei database tradizionali: i dati non vengono conservati in uno o più server ma sussiste un rapporto paritario tra nodi[194], reso possibile dall'impiego di reti "peer-to-peer e dalla crittografia[195]. È di facile intuizione la portata rivoluzionaria di questo primo requisito: per la prima volta i soggetti che operano a diverso titolo nel

---

[192] Sul tema, in particolare, v. BEVILACQUA, *Le varie tipologie di blockchain*, in BATTAGLINI, GIORDANO (a cura di), *Blockchain e smart contracts*, Milano, 2019, 56 ss.; RAMPONE, *Ecologia delle parole e blockchain*, in *Associazione Blockchain Italia*, 2019, disponibile al seguente link: *https://associazioneblockchain.it/doc/ecologia-delle-parole-e-blockchain/*

[193] Le sei caratteristiche principali sono illustrate in *La Blockchain spiegata semplice, Definizioni, funzionamento, applicazioni e potenzialità*, in *osservatori.net* a cura del Politecnico di Milano *https://blog.osservatori.net/it_it/blockchain-spiegazione-significato-applicazioni*

[194] I nodi sono costituiti fisicamente dai server di ciascun partecipante.

[195] Per ulteriori approfondimenti sul tema v. WRIGHT, DE FILIPPI, *Decentralized Blockchain Technology and The Rise of Lex Cryptographia*, in *Social Science Research Network*, 2015, http://papers.ssrn.com/abstract=2580664, 4-5.

sistema non ripongono la propria fiducia nella solidità e attendibilità di un ente centrale che funge da intermediario ma nella piattaforma in sé e nel modo in cui viene concepita.

È in questa prospettiva che viene in gioco il secondo elemento definitorio della *blockchain*, vale a dire la decentralizzazione. Le informazioni immesse nel registro vengono dapprima registrate e contestualmente distribuite tra più nodi indipendenti tra loro; questo meccanismo è stato ideato a garanzia della sicurezza informatica dell'infrastruttura in quanto la compromissione di un singolo nodo non è idonea ad intaccare gli altri e, di conseguenza, l'integrità dell'insieme dei dati registrati.

Le ulteriori tre caratteristiche sono state pensate a garanzia dell'affidabilità dell'intero sistema. In primo luogo, la tracciabilità dei trasferimenti attraverso un meccanismo che garantisce la possibilità di verificare sempre la provenienza dei dati immessi nel registro; in secondo luogo, la trasparenza del registro, che rende il contenuto visibile nonché facilmente consultabile[196]; in terzo luogo, l'immutabilità della *blockchain*, tale per cui una volta iscritti del registro distribuito, i dati non possono essere modificati senza il consenso del sistema.

E' nella programmabilità dei trasferimenti che si individua il sesto ed ultimo requisito della blockchain. Quest'ultimo fa riferimento alla possibilità di pianificare il compimento automatico di azioni specifiche al verificarsi di condizioni predeterminate[197].

Alla luce delle caratteristiche sopra illustrate, la *blockchain* è da considerarsi come una delle scoperte più rivoluzionarie dello scorso decennio, al pari dell'invenzione di internet negli anni Novanta del Novecento. La stessa, concepita come un'infrastruttura disintermediata, decentralizzata, sicura, trasparente ed immutabile è in grado di ridefinire il

[196] Una copia di ciascun *ledger (*registro pubblico nel quale vengono annotate in modo immutabile, trasparente e sequenziale tutte le transazioni effettuate), è conservata a cura di ciascun nodo della rete.

[197] Tale potenzialità si pone a fondamento degli *smart contracts*, una declinazione della tecnologia di *blockchain* che sarà oggetto di un'analisi specifica nel sottoparagrafo che segue.

modo in cui effettuiamo transazioni, archiviamo le informazioni e condividiamo i dati[198].

Se in un primo momento il suo impiego era limitato al solo ambito finanziario, ad oggi molti più settori[199] stanno iniziando ad usufruire dei benefici derivanti dalla stessa[200]; basti pensare al contributo offerto dalla tecnologia in esame alla gestione della *supply chain* che, anche a causa della globalizzazione, è diventata sempre più articolata e complessa[201], nonché ai benefici apportati al mercato delle energie rinnovabili dove la *blockchain* è impiegata per la creazione di piattaforme *peer-to-peer* che consentono agli utenti di comprare e vendere energia senza la necessaria presenza di un terzo intermediario[202] In ultimo sono da menzionare i suoi molteplici impieghi in ambito governativo e della pubblica amministrazione.[203]

Il principale avversario allo sviluppo delle tecnologie di *blockchain* è rappresentato dalla frammentarietà delle discipline legislative vigenti e dall'assenza di una cornice normativa unitaria e armonica a livello comunitario; ne conseguono incertezza nel diritto, carenza di fiducia tra i potenziali beneficiari e assenza di interoperabilità tra le diverse declinazioni di registro distribuito. Stabilire regole universali per l'accesso e il funzionamento della *blockchain* rappresenta pertanto un presupposto fondamentale per garantire uno suo impiego sicuro, trasparente e rispettoso

[198] Secondo una previsione del *World Economic Forum*, entro il 2027 il 10% del PIL globale sarà su Blockchain. Sul punto v. BIANCHI, *Investire attraverso i security token, entro il 2023,* in CETIF, 2022 *https://www.cetif.it/about-us-they-say/investire-attraverso-i-security-token-entro-il-2023*

[199] Sul punto v., PORTALE, *Le applicazioni della Blokchain: i 5 settori più promettenti*, in *Osservatori.net*, 2019 *https://blog.osservatori.net/it_it/applicazioni-blockchain*

[200] Il Parlamento europeo nel febbraio del 2017 ha pubblicato un report che evidenzia gli ambiti in cui la tecnologia di blockchain può avere maggiore impatto, v. BOUCHER, *How blockchain technology could change our lives*, in *European Parliamentary Research Service*, 2017, 6 ss.;

[201] Per *supply chain* si intende l'intero procedimento che consente di immettere nel mercato un prodotto o un servizio, trasferendolo dal produttore al cliente. Grazie all'impiego della *blockchain,* è possibile garantire maggiore trasparenza, sicurezza e tracciabilità dei prodotti all'interno della stessa.

[202] *Power Ledger* rappresenta un esempio concreato di piattaforma globale di *trading* di energia basata sulla tecnologia *blockchain*

[203] Uno dei maggiori impieghi in questo settore attiene alla creazione di un'identità digitale al fine di automatizzare l'accesso ai servizi pubblici, velocizzare le procedure e snellire la burocrazia: un esempio concreto è rappresentato da CIVIC, una piattaforma che si avvale della tecnologia a registro distribuito per gestire l'identità degli utenti *https://www.civic.com/*

dei diritti fondamentali nonché una delle sfide più ambizione in capo all'Unione Europea. [204]

Nell'ultimo quinquennio si stanno susseguendo una serie di proposte e attività in ambito europeo volte a sanare la suddetta lacuna[205]: di seguito un elenco delle principali iniziative seguendo l'ordine predisposto dal sito ufficiale dell'Unione europea[206].

A partire dal 2018, nel contesto del mercato unico europeo, la Commissione ha avviato i lavori per lo sviluppo di una proposta di regolamentazione dei mercati delle cripto-attività (MICA) che attualmente è in fase di discussione da parte del Parlamento europeo e del Consiglio[207]. Quest'ultima costituisce un'iniziativa nel più ampio pacchetto finanziario digitale adottato dalla Commissione in data 24 settembre 2020 ed indirizzato ad elaborare una strategia aggiornata in materia di finanza digitale e *retail*. In aggiunta, il 3 giugno 2021 è stata pubblicata da parte della Commissione europea una proposta di regolamento volta a modificare il regolamento UE n. 910/2014[208]. L'obiettivo è quello istituire sia un'identità digitale europea (eIDAS2) attraverso la predisposizione di un nuovo servizio fiduciario per i registri elettronici che un c.d. «*European Digital Identity Wallet*»[209].

Al fine di predisporre gli *standard* necessari a favorire uno sviluppo omogeneo delle tecnologie a registro distribuito nel territorio dell'Unione, la Commissione, a partire da settembre 2017, ha dato il via ad un susseguirsi di seminari sul tema, utili a riunire le principali organizzazioni per lo sviluppo delle linee guida, i consorzi attivi nell'opera di standardizzazione

---

[204] Sul tema v. *Blockchain and Distributed Digital Ledger Technologies,* 2023 *https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/blockchain-and-distributed-ledger-technologies-0*

[205] In argomento v. SIMBULA, *Normativa italiana sulle DLT*, in BATTAGLINI, GIORDANO (a cura di), *Blockchain e Smart contracts*, Milano, 2019, 135 ss.

[206] V. *Blockchain and Distributed Digital Ledger Technologes,* 2023, cit.

[207] COM/2020/593 final

[208] V. Proposal for a regulation of the European parliament and of the council amending Regulation (EU) No 910/2014, COM/2021/281 final

[209] Vale a dire un portfolio digitale personale a disposizione dei cittadini e dei residenti nel territorio dell'Unione Europea che funga da mezzo di identificazione degli stessi. *https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en*

internazionale delle tecnologie a registro distribuito, le parti interessate a vario titolo ed i rappresentanti dei partenariati pubblico-privati.

Sempre con l'obiettivo di creare un contesto di collaborazione tra gli addetti ai lavori e scongiurare il rischio di emersione di norme contrastanti, in data 17 giugno 2020 la Commissione europea ha organizzato il *webinar* «*Joining Forces for Blockchain Standardization*»[210] che ha visto la partecipazione di oltre quattrocento esperti provenienti da tutto il mondo, riuniti per discutere dei progressi nel processo di standardizzazione in materia di identità digitale, interoperabilità, *governance* e *smart contacts*[211].

Per perseguire la medesima finalità, la Commissione europea ha istituito una serie di tavole rotonde denominate «*ICT Verticals and Horizontals for Blockchain Standardization*».[212] Queste ultime, tenutesi tra la seconda metà del 2020 e nell'inizio del 2020, si sono occupate di dieci gruppi tematici principali[213] e hanno contribuito allo sviluppo di oltre settanta progetti finanziati da *Horizon 2020*[214].

In aggiunta, nel febbraio 2028, la Commissione europea ha fondato l'Osservatorio e *Forum* dell'UE sulla *blockchain*[215], anch'esso utile a coinvolgere le parti interessate private e le autorità pubbliche nelle discussioni tecniche e normative sullo sviluppo e sulle applicazioni della tecnologia *blockchain*.

---

[210] V. *https://ec.europa.eu/digital-single-market/en/news/joining-forces-blockchain-standardisation*

[211] In quest'occasione è stato altresì condotto un sondaggio per identificare i settori più critici, che necessitano una maggiore coesione tra le parti interessate: l'interoperabilità è risultata l'area più bisognosa di un approccio collaborativo, seguita dall'identità, dai contratti intelligenti, dalla governance e in ultimo dalla sicurezza.

[212] Per un approfondimento su tema v. *https://digital-strategy.ec.europa.eu/en/events/ict-verticals-and-horizontals-blockchain-standardisation*

[213] I dieci gruppi tematici sono: *Fintech, Digital Assets* e reti intelligenti; Società digitale, identità e *privacy*; economia digitale, PMI, industria e *supply chain*; sicurezza informatica; *Internet of things*; sanità elettronica; *future Internet, media e big data*; obiettivi di sviluppo sostenibile; *smart contracts* ed intelligenza artificiale.

[214] *Horizon 2020* è stato il programma di finanziamento della ricerca e dell'innovazione dell'UE per il periodo 2014-2020 che contemplava un budget di quasi 80 miliardi di euro. Allo stesso è succeduto *Horizon EuropeEN•••*

[215] L'Osservatorio è costituito dai maggiori esperti europei in materia che collaborano attivamente attraverso l'organizzazione di workshop tematici e la produzione di report utili a supportare gli stakeholders nell'implementazione dei servizi basati sulla *blockchain* in Europa.

Una delle principali iniziative messe in campo dall'UE ha avuto luogo il 10 aprile 2018 ed ha visto l'istituzione dell'*European Blockchain Partnership (EBP):* i ventisette paesi membri insieme alla Norvegia e il Liechtenstain hanno redatto una dichiarazione congiunta che li impegna a cooperare per la creazione di un'infrastruttura europea di servizi *blockchain* (EBSI)[216] finalizzata a sostenere l'erogazione di servizi pubblici transfrontalieri attraverso l'interoperabilità e nel rispetto dei più alti *standard* di sicurezza.

Un anno dopo rispetto alla nascita della *partnership* europea illustrata, la Commissione ha sostenuto il lancio *dell'International Association of Trusted Blockchain Applications* (INATBA)[217]. Un *forum* a livello globale che consente agli sviluppatori e agli utenti di DLT di interagire con gli esponenti nell'ottica di sviluppare linee guida a favore dell'interoperabilità e *standard* globali volti a migliorare i servizi digitali.
L'ultima iniziativa partorita dalla Commissione europea ha visto la predisposizione in data 14 febbraio 2023 di uno spazio di sperimentazione e consulenza in materia *blockchain*[218], in attuazione del programma Europa digitale [219]. Si tratta di un ambiente sicuro, anche chiamato *sandbox*, utile alle imprese per testare prodotti e servizi, richiedere consulenza giuridica e dialogare con le autorità di regolamentazione competenti, il tutto a garanzia della certezza del diritto.

Quanto all'impiego della tecnologia *blockchain* in Italia, un *report* del 2020 stilato dalla OECD[220] illustra come nel nostro paese la diffusione di soluzioni tecnologiche basate sul registro distribuito si stia moltiplicando progressivamente, in particolare nei settori quali la gestione della *supply chain*, la protezione del *copyright* e le risorse umane. Alla luce dei dati

[216] Per un approfondimento sul punto consultare: *https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home*
[217] V. *https://inatba.org/*
[218] V. *https://www.eublockchainforum.eu/news/launch-european-blockchain-regulatory-sandbox*
[219] Sul tema consulta il *link*: *https://digital-strategy.ec.europa.eu/en/activities/digital-programme*
[220] Il report è intitolato "*Blockchain for Small-Medium Sized Enterprise and entrepreneurs in Italy*" ed è stato realizzato dall'Organizzazione per la cooperazione e lo sviluppo economico. *https://www.oecd-ilibrary.org/economics/blockchain-for-smes-and-entrepreneurs-in-italy_f241e9cc-en;jsessionid=o2CRzbQYEPFT3G_Kol5cY0c1f5UN1QO4GQVch51Z.ip-10-240-5-35*

raccolti[221], l'Organizzazione per la cooperazione e lo sviluppo economico ha concluso che la nostra nazione ha il potenziale per conquistarsi un ruolo da protagonista in questo mercato che va prendendo forma. Conduce al medesimo risultato l'analisi condotta dal Politecnico di Milano[222] che colloca l'Italia tra i dieci paesi al mondo per diffusione di progetti basati sulla tecnologia blockchain nel 2019[223].

5.1 Gli *smart contracts*

Gli *smart contracts* consistono in programmi *software* che basano il loro funzionamento sulla tecnologia dei registri distribuiti. In realtà, l'idea di predisporre un contratto intelligente nasce in maniera del tutto svincolata dalla *blockchain*. Il primo esempio di *smart contracts*, infatti, ha preso piede a partire degli anni Settanta del Novecento e le prime sperimentazioni in materia risalgono agli anni Novanta del secolo scorso, quando ancora la tecnologia a registro distribuito non era stata affatto teorizzata[224].

L'intuizione di basare il funzionamento dei *software* in questione su tecnologie DLT deriva dall'esigenza di assicurare trasparenza, sicurezza, fiducia e immodificabilità degli stessi, senza il bisogno di affidarsi a soggetti terzi esperti in materie giuridiche. È grazie all'impiego della *blockchain* a supporto dei programmi che si è passati dalla più basilare idea di contratto automatizzato, ancora bisognoso dell'intervento di un intermediario, all'elaborazione di contratti eseguibili in via del tutto automatica ed autonoma[225].

---

[221] Ammontano a 25,6 milioni di euro i fondi stanziati nel mercato della blockchain e sono 67 i *blockchain solution providers* e le *startups* nel settore

[222] Per un approfondimento sul puto v. *https://www.som.polimi.it/event/osservatorio-blockchain-distributed-ledger-170120/*

[223] L'investimento totale da parte delle imprese italiane ammonta a circa 30 milioni di euro, il 100% in più rispetto all'anno precedente.

[224] L'idea originaria atteneva all'esigenza di gestire l'attivazione o disattivazione di una licenza software al verificarsi di condizione predeterminate, si trattava di fatto di uno *smart contract ante litteram*, in una forma più semplificata. Sul punto v. BELLINI, *Smart Contracts: che cosa sono, come funzionano quali sono gli ambiti applicativi*, in *Blockchain4innovation*, 2018 *https://www.blockchain4innovation.it/mercati/legal/smart-contract/blockchain-smart-contracts-cosa-funzionano-quali-gli-ambiti-applicativi/*

[225] In argomento v. EUBLOCKCHAIN OBSERVATORY AND FORUM, *Smart Contracts*, 2022, 5 *https://www.eublockchainforum.eu/*.

La locuzione *smart contract* è stata coniata per la prima volta nel 1996 dall'informatico nonché teorico del diritto Szabo e fa riferimento a protocolli di transazione computerizzati progettati alla luce di principi giuridici, teorie economiche e tecnologiche, in grado di eseguire i termini di un contratto.[226]

Tutt'ora non esiste un'unica definizione generalmente condivisa di *smart contracts*, una delle più recenti e attendibili risulta essere quella contenuta al comma 2 dell'art 8 ter, contenuto nel d.l. 135/2018 che oltre a ribadire l'impiego delle tecnologie DLT nel funzionamento del *software*, precisa che i contratti intelligenti consistono in programmi capaci di vincolare due o più parti alla luce degli effetti predefiniti dalle stesse, previo soddisfacimento della forma scritta e previa identificazione informatica dei soggetti interessati nel rispetto dei requisiti fissati dalle linee guida pubblicate dall'Agenzia per l'Italia digitale.

Effettuando un'operazione di sintesi tra le diverse teorie che si avvicendano[227], è possibile concludere che gli *smart contracts* costituiscono contratti supportati da *software* che si avvalgono della *blockchain*, la cui esecuzione avviene automaticamente al verificarsi di condizioni prestabilite dalle parti che ne risultano vincolate.

Per la creazione[228] di un contratto intelligente occorre dapprima tradurre le clausole contrattuali in un protocollo informatico[229]. Segue la programmazione dello stesso a cura delle parti interessate che consiste principalmente nell'individuazione della condizione al verificarsi della quale il codice algoritmico porrà in essere un'operazione specifica, che il più delle volte consiste nella conclusione del contratto, nell'esecuzione dello stesso o di una o più clausole contrattuali.

---

[226]Definizione di *smart contract* in SZABO, *Smart Contracts: Building Blocks for digital market, 1996, «http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html. »*.

[227] Per un approfondimento sul tema v. MIK, *Smart Contracts: Terminology, Technical Limitations and Real-World Complexity*, in *SSRN*, 2017, 3 ss.

[228] Il procedimento di creazione di uno *smart contract* è stato illustrato da Vitalik Buterin, co-fondatore di *Etereum*, in occasione di un *summit* sulla *blockchain* tenutosi nel 2014. L'intervento è disponibile al seguente indirizzo: *https://www.youtube.com/watch?v=TDGq4aeevgY*

[229] Si tratta di codice algoritmico che opera alla luce dello schema logico ITTT, un acronimo che sta per "*if this than that*", tradotto "se si verifica questo allora accade quello".

Quanto ai benefici derivanti dall'impiego dei contratti intelligenti in luogo di quelli tradizionali, già nell'idea iniziale dell'ideatore Szabo, questi ultimi sarebbero dovuti consistere nel soddisfacimento automatico di condizioni contrattuali comuni, nella riduzione al minimo delle eccezioni sia dannose che accidentali e nella minimizzazione della necessità di intermediazioni fiduciarie[230].

Ad oggi l'utilità di avvalersi di uno *smart contract* è riconducibile ad una serie di caratteristiche principali che connotano gli stessi[231]. Prime fra tutti la velocità e l'efficienza: gli smart contracts, infatti, grazie all'alto grado di automazione, garantiscono una semplificazione dell'intero ciclo di vita di un contratto[232].

In secondo luogo, la trasparenza: gli *smart contracts* garantiscono un maggior livello di chiarezza rispetto al prototipo tradizionale e limitano le possibilità di corruzione, dal momento in cui per ogni modifica che si intende fare al contratto è richiesto il consenso di tutte le parti coinvolte.
Ulteriore punto di forza dei contratti intelligenti è rappresentato dalla loro indipendenza da intermediari per l'esecuzione, ne consegue un minor rischio di manipolazione dello stesso e un notevole risparmio di spesa.

In ultimo la sicurezza: grazie all'uso della crittografia dei dati, i contratti intelligenti sono a prova di manomissione e rappresentano un'alternativa altamente sicura ai contratti cartacei. In aggiunta, essendo costituiti da porzioni di codici algoritmici, offrono il vantaggio di essere facilmente riutilizzati per operazioni simili alla sola introduzione di modifiche minime.

La sicurezza dei contratti intelligenti è altresì garantita da piattaforme ad hoc come la *Open Zeppelin*[233], la *Why3*[234] e la *Oyente*.[235]

---

[230] SZABO, *Smart Contracts*, 1996, cit.
[231] Sul punto v. EUBLOCKCHAIN OBSERVATORY AND FORUM, *Smart Contracts*, cit., 7 ss.; CARBONE, *Smart contracts: caratteristiche tecniche e tecnologiche*, in BATTAGLINI, GIORDANO (a cura di), *Blockchain e Smart contracts*, Milano, 2019, 237 ss.
[232] Pagamenti automatizzati, richieste di risarcimento immediate, razionalizzazione nella gestione dei dati nonché una maggiore efficienza nella supply chain rappresentano solo alcuni dei vantaggi derivanti dall'impiego dei contratti intelligenti.
[233] Per approfondirne il funzionamento v. *https://www.openzeppelin.com/*
[234] Per maggiori informazioni v. *https://why3.lri.fr/*
[235] Il sito ufficiale è consultabile al seguente *link*: *https://oyente.tech*

Illustrata la definizione di contratto intelligente ed evidenziate le caratteristiche principali, è utile fornire una panoramica delle norme vigenti in materia sia in ambito nazionale che europeo.

In data febbraio 2019, il Parlamento italiano ha convertito il d.l. 135/2018 nella l. 12/2019, anche noto come decreto semplificazioni. Tale provvedimento, oltre ad illustrare per la prima vola la definizione di tecnologie DLT[236], ha introdotto due importanti novità.

In primo luogo, ha stabilito che la registrazione di un documento elettronico all'interno di un registro distribuito produce gli stessi effetti giuridici della convalida temporale elettronica contemplata dal regolamento UE n. 910/2014. In secondo luogo, ha per la prima volta riconosciuto gli *smart contracts* e la loro piena validità legale[237].

A livello comunitario, la Commissione europea ha predisposto una proposta di regolamento[238] volta ad armonizzare le norme sull'accesso ai dati e sull'utilizzo degli stessi, con l'obiettivo ultimo di costituire un mercato unico e di rendere l'Europa una *leader* nell'economia dei *big data*[239].
Il suddetto testo normativo contiene una definizione puntuale degli *Smart Contracts*[240] nonché la loro disciplina[241] che fa leva sulle diverse potenzialità degli stessi, prima fra tutte la garanzia che le condizioni contrattuali stabilite dalle parti vengano rispettate in virtù della tecnologia di cui si avvalgono.

La proposta di regolamento individua altresì nelle quattro caratteristiche delineate dall'art. 30 del *Data Act* i requisiti essenziali che ogni *smart contract* deve integrare.

Il primo elemento è rappresentato dalla robustezza: è necessario garantire che il contratto intelligente venga progettato in modo da offrire un grado molto elevato di solidità, così da scongiurare errori di sistema e

[236] Si rimanda a quanto già illustrato nel paragrafo precedente
[237] Sul punto v. EUBLOCKCHAIN OBSERVATORY AND FORUM, *Smart Contracts*, cit., 21
[238] La proposta di regolamento risale al febbraio 2022 e prende il nome di *Data Act*
[239] il processo legislativo in seno al Parlamento europeo e al Consiglio è attualmente in corso
[240] I contratti intelligenti vengono definiti come programmi informatici su registri elettronici distribuiti che eseguono e predispongono transazioni in base a condizioni predeterminate
[241] V. art. 28 par. 1 lett. d e art 29 del *Data Act*.

resistere alla manipolazione da parte di terzi. La possibilità di risoluzione e interruzione sicura dello stesso costituisce il secondo requisito: si richiede pertanto la presenza di un meccanismo idoneo a reimpostare lo *smart contract* in modo da porre fine all'esecuzione automatica di transazioni indebite. La terza caratteristica contemplata dal *Data Act* è quella della verificabilità': è consigliato archiviare e conservare i dati contenuti nel contratto al fine di tenere traccia delle operazioni poste in essere sugli stessi.

In ultimo, il controllo degli accessi: un contratto intelligente deve essere protetto attraverso rigorosi meccanismi idonei a verificare chi si sia avvalso degli stessi, con l'obiettivo di evitare manomissioni illegittime dello stesso.

Alla luce di quanto delineato finora, risulta chiaro quanto quelli della velocità, dell'efficienza, della trasparenza, della sicurezza e dell'immutabilità rappresentino dei connotati rivoluzionari per un sistema digitale. Le tecnologie a registro distribuito quali, in modo particolare, la *blockchain* e gli *smart contract*, se già offrono un contributo notevole in ambito finanziario, a supporto della pubblica amministrazione e nel settore agroalimentare[242], potrebbero essere validamente impiegati altresì per la costruzione di un modello organizzativo alla luce delle indicazioni fornite dal decreto 231 del 2001 e delle principali *best practices* elaborate in materia.

Gli stessi offrono infatti la possibilità di tenere traccia delle attività interne, archiviare il contenuto dei flussi informativi nonché gestire le risorse finanziarie nella disponibilità dell'ente in maniera sicura e trasparente, così da perfezionare la capacità preventiva di un MOG e di ridurre al minimo il rischio di verificazione di un reato all'interno dell'ente[243].

---

[242] Stando a quanto riportato dal contributo pubblicato nel 2019 a cura dell'Osservatorio.net gestito dal Politecnico di Milano, sul punto v. *https://blog.osservatori.net/it_it/applicazioni-blockchain*; GHIANI, *Blockchain: linee guida*, cit. 17 ss.

[243] Una panoramica degli utilizzi delle tecnologie DLT a supporto della *compliance* penale verrà offerta nel secondo capitolo del presente lavoro di ricerca

CAPITOLO II
DIGITAL CRIMINAL COMPLIANCE: OPPORTUNITÀ E CONCRETA APPLICAZIONE

1. Le opportunità della *Digital Criminal Compliance*

La portata trasformativa delle nuove tecnologie[1] ha avuto un impatto notevole non solo in ogni ambito della società ma anche nei confronti della giustizia, incluso il diritto penale[2]. L'incontro tra il diritto e l'intelligenza artificiale, accomunati dalla loro ragion d'esistere e dal connotato della pervasività nelle vite dei cittadini, è stato considerato da alcuni giuristi come «ineludibile»[3] ed è proprio così che si è rivelato anche nella prassi.

In realtà, l'idea di sfruttare i nuovi paradigmi tecnologici nelle diverse branche del diritto è relativamente recente. Quest'ultima, infatti, è già rinvenibile nelle pubblicazioni di autorevole dottrina anglosassone risalenti agli anni Novanta del secolo scorso[4] che hanno dato il via al florido dibattito tra gli studiosi del diritto in merito alle diverse potenzialità nonché agli altrettanti rischi derivanti dall'utilizzo dei *tools* intelligenti nel settore della giustizia.

Un'analisi dei contributi poc'anzi citati consente di prendere atto che i primi ambiti in cui è risultato utile avvalersi dei nuovi paradigmi tecnologici hanno riguardato le procedure amministrative. Queste ultime, infatti, richiedono l'applicazione di regole chiare a fatti non controversi, ben conciliandosi con il *modus operandi* degli algoritmi di IA, i quali, a partire

[1] Sul punto si rimanda a quanto delineato del capitolo 1 del presente contributo

[2] Cfr. v., SABIA, *Artificial intelligence and environmental criminal Compliance,* cit.,179; QUATTROCOLO, *Qualcosa di meglio del diritto (e del processo) penale?*, in *disCRIMEN*, 2020, 2; MORGANTE, FIORINELLI, *Promesse e rischi della compliance penale digitalizzata*, in Arch. Pen, 2022, 2.

[3] Sul punto v. UBERTIS, *Intelligenza artificiale, giustizia penale,* cit., 2.

[4] Di seguito i principali testi che hanno affrontato il tema dell'utilizzo delle nuove tecnologie nel campo della gistizia, evidenziandone le opportunità ed i rischi v. WEIZENBAUM, *Computer Power and Human Reason*, San Francisco, 1976; GARDNER, *An Artificial Intelligence Approach to Legal Reasoning*, Cambridge, 1987; BERMAN, HAFNER, *The Potential of AI to Help Solve the Crisis in our Legal System*, in CACM, vol.32(8), 1989, 928 ss; PETHE, RIPPEY, KALE, *A Specialized Expert System for Judicial Decision Suppor*t, In *Proceedings of the Second International Conference on Artificial Intelligence and Law*, New York, 1989, 190 ss; BRANTING, *An Issue-Oriented Approach to Judicial Document Assembly*, In *Proceedings of the Fourth International Conference on Artificial Intelligence and Law*, New York, 1993, 228 ss.

da un *input* fornito dal programmatore o ricavato dal *web*, consentono di elaborare un preciso *output.*

Negli anni successivi, tuttavia, gli studi in materia si sono concentrati sempre di più sullo sfruttamento delle nuove tecnologie in settori più complessi nonché caratterizzati da più ampi margini di discrezionalità, quali, in modo particolare, il processo decisionale giudiziario.

Seppur con un decennio di ritardo, anche nel nostro Paese gli studiosi del diritto hanno iniziato a prendere in considerazione le diverse opportunità e agli altrettanti rischi connessi all'impiego dei nuovi *tools* nel campo della giustizia. Alcuni autori si sono spinti addirittura ad affermare che la semplificazione della giustizia rappresenti uno dei fini ultimi che l'intelligenza artificiale intende perseguire[5].

È possibile individuare quattro ambiti principali in cui si è prospettata la possibilità di avvalersi delle nuove tecnologie[6].

Primo fra tutti è l'utilizzo dell'IA nell'attività di *law enforcement*[7] e polizia predittiva che, ormai da qualche anno, costituisce una solida realtà anche nel nostro Paese[8]: i *software* si configurano come strumenti utili alle forze dell'ordine nella gestione della mole di dati a disposizione della stessa, nell'analisi di immagini e video, nelle attività di riconoscimento facciale ed identificazione biometrica ed, infine, nell'individuazione delle zone più a rischio di commissione di reato e dei soggetti più propensi a delinquere[9].

---

[5] Cfr. ROMANO, *Diritto, robotica e teoria dei giochi: riflessioni su una sinergia*, in ALPA (a cura di), *Diritto e intelligenza artificiale*, Pisa, 2020, 105.

[6] Una panoramica esaustiva è presente in BASILE, *Intelligenza artificiale e diritto penale: quattro possibili percorsi d'indagine*, in *Dir. Pen e Uomo*, 2022, 2 ss.

[7] Per un approfondimento a riguardo v. FERGUSON, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, New York, 2017, 3 ss; HARRY, SURDEN, *Artificial Intelligence and Law: An Overview*, vol. 35, Ga. St. U. L. Rev, 2019, 1333 ss. *https://readingroom.law.gsu.edu/gsulr/vol35/iss4/8*

[8] In Italia sono stati sviluppati due strumenti principali: il *Key Crime* e l'*X-Law*. Il primo è stato adottato dalla Questura di Milano in relazione ai reati che presentano il requisito della serialità: si tratta infatti di un modello matematico idoneo a prevenire il tempo e il luogo in cui verrà commesso un crimine alla luce delle informazioni inerenti alla prima manifestazione criminosa, sul punto v. MORABITO, *La chiave del crimine*, in *Poliziamoderna*, 2015, 36 ss.

Il secondo consiste in un software ideato dalla Questura di Napoli e completato dal Dipartimento di Pubblica Sicurezza del Ministero dell'Interno per implementare la sicurezza urbana. Per comprenderne le modalità di funzionamento v. *https://www.xlaw.it/presentazione/*

[9] Così si legge nel Documento di presentazione redatto dall'OSCE in occasione dell'*Annual Police Experts Meeting* "*Artificial Intelligence and Law Enforcement: An Ally or an Adversary?*", tenutosi il 23 e 24 Settembre 2019 a Wien.

In secondo luogo, ampliamente diffuso negli Stati Uniti e solo caldeggiato nei Paesi europei è l'utilizzo degli algoritmi "intelligenti" per quantificare il rischio che un soggetto integri una fattispecie criminosa, i c.d. *Risk assesment tools*[10]. Si tratta di strumenti capaci di elaborare una percentuale di propensione al rischio ben precisa, risultante dall'analisi di informazioni personali del soggetto quali, a titolo esemplativo, quelle relative al contesto familiare, alla situazione economico sociale e al luogo di dimora.

Il terzo ambito in cui le nuove tecnologie hanno rivestito un ruolo di notevole impatto attiene allo svolgimento del processo giudiziario. Si è prospettato infatti l'utilizzo delle stesse a supporto dell'autorità giudiziaria nella redazione di atti, nella formazione delle prove e nella previsione circa l'esito di un giudizio[11], in quel processo articolato che prende il nome di giustizia predittiva[12].

L'impiego dei nuovi *tools* in questo frangente, se da un lato risulta utile a rendere l'intero processo giudiziario più veloce ed economico nonché improntato alla calcolabilità e alla prevedibilità[13], dall'altro determina il rischio di violazione di molteplici principi fondamentali propri del diritto penale, primo fra tutti il libero convincimento dell'autorità giudiziaria[14].

Già i primi studiosi del diritto anglosassone avevano optato per un approccio cauto in materia, dimostrandosi consapevoli della necessità che il

---

[10] Sul punto v. CANZIO, *Il dubbio e la legge*, in *Diritto penale contemporaneo*, 2018, 1 ss; GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assesment tools tra Stati uniti ed Europa*, in *Dir. Pen. Cont*., 3 ss; CASTELLI, PIANA, *Giustizia predittiva. La qualità della giustizia in due tempi*, in *Questione Giustizia*, 2018, 153 ss.

[11] Cfr. ARDUINI, *La "scatola nera" della decisione giudiziaria: tra giudizio umano e giudizio algoritmico*, in *BioLaw Jurnal*, 2021, 456;

[12] "Per giustizia predittiva deve intendersi la possibilità di prevedere l'esito di un giudizio tramite alcuni calcoli; non si tratta di predire tramite formule magiche, ma di prevedere la probabile sentenza, relativa ad uno specifico caso, attraverso l'ausilio di algoritmi. Il diritto può essere costruito come una scienza, che trova la sua principale ragione giustificativa nella misura in cui è garanzia di certezza: il diritto nasce per attribuire certezza alle relazioni umane, tramite una complessa attribuzione di diritti e doveri", definizione contenuta in Enciclopedia Treccani.
Parte della dottrina è convinta che l'automazione del processo decisionale consenta di ottenere vantaggi di non poco conto, sul punto v. CASTELLI, PIANA, *Giustizia predittiva. La qualità della giustizia in due tempi*, in *Quest. Giust. Trim*., 157 ss; BARATTELLI, *Giustizia predittiva, decisione robotica e ruolo del giudice*, in *Giust. Civ*., 2020, 281 ss.

[13] Di quest'avviso già SARTOR, BRANTING, *Introduction: judicial applications of artificial intelligence*, in *Artificial intelligence and law*, 1998, 110.

[14] Principio contemplato nel nostro ordinamento giudiziario dal co. 1 art 192 c.p.p.

processo giuridico decisionale restasse di sola competenza delle persone fisiche[15]. Questa convinzione è maturata sia alla luce dell'ontologica complessità dello stesso, il quale implica la valutazione del compendio di prove fornite dalle parti, l'interpretazione della legge, la valutazione circa la credibilità dei testimoni e l'irrogazione di una pena[16] che in relazione al notevole impatto che le decisioni incardinate nelle sentenze hanno sulle vite dei cittadini.

Per le ragioni sopra illustrate, piuttosto che ambire alla creazione di un "giudice automatico" capace di sostituirsi all'autorità giudiziaria persona fisica, i progetti di ricerca in materia si sono concentrati sullo sviluppo di strumenti tecnologici a supporto delle attività giudiziarie, con l'obiettivo meno rischioso di facilitarne lo svolgimento[17].

Sulla stessa linea d'onda si collocano gran parte dei contributi dottrinali pubblicati sul tema nel nostro Paese[18]. Le perplessità avanzate dagli studiosi del diritto in relazione all'utilizzo degli algoritmi predittivi nel corso del procedimento giudiziale sono principalmente due[19]: la prima attiene all' inevitabile influenza che gli esiti forniti dal *tool* "intelligente" andranno ad esercitare sull'autorità giudiziaria, la quale sarà portata ad optare per la decisione standardizzata offerta dal *software,* con il rischio di non dare rilievo alle peculiarità del caso concreto, la seconda fa riferimento al rischio di incorrere nei *bias* di cui il «software giudicante»[20] è fisiologicamente caratterizzato nonché nei «*bias dei bias*»[21], vale a dire l'insieme dei pregiudizi intrinseci agli *input* forniti dall'uomo alla macchina[22], profili entrambi idonei ad inquinare l'*output* prodotto dalla

[15] V. BRANTING, *An Issue-Oriented Approach*, in *Proceedings of the Fourth International Conference*, cit., 228 ss.
[16] a sua volta derivante dalla contemperazione tra esigenza punitiva a quella rieducativa
[17] V. PETHE, RIPPEY, KALE, *A Specialized Expert System for Judicial Decision Suppor*t, cit., 190 ss.
[18] Cfr. CASTELLI, PIANA, *Giustizia predittiva. La qualità della giustizia in due tempi*, cit., 54 ss.
[19] In argomento v. TREZZA, *L'Intelligenza Artificiale come ausilio alla standardizzazione del modello 231: vantaggi "possibili" e rischi "celati",* in *Giurisprudenza Penale Web*, 2021, 3.
[20] Espressione utilizzata da TREZZA, *L'Intelligenza Artificiale come ausilio alla standardizzazione,* cit., 3.
[21] Sul punto ancora TREZZA, *L'Intelligenza Artificiale come ausilio alla standardizzazione,* cit., 3.
[22] Ne è un esempio calzante il caso LOOMIS negli Stati Uniti v. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale*, cit., 6 s.

macchina al termine delle operazioni di raccolta, analisi e studio dei dati a disposizione[23].

Infine, già realtà per diverse *corporations* stabilite nei Paesi anglosassoni e solo di recente oggetto dei dibattiti dottrinali nel nostro Paese è l'impiego delle nuove tecnologie a supporto della *compliance*[24] interna all'ente[25], vale a dire l'insieme variegato di misure organizzative adottate da una persona giuridica al fine di scongiurare il rischio di non conformità a regole, divieti, principi e linee guida in vigore. Fenomeno che negli ultimi anni ha assunto una sempre maggiore centralità, tanto da costituire l'obiettivo ultimo a cui mirano i sistemi di responsabilità delle persone giuridiche elaborati nei paesi anglosassoni[26] e rappresentare il vero cardine del sistema normativo delineato dal d.lgs 231/2001[27].

Un'analisi della prassi in materia dimostra che sempre più imprese private con sede negli Stati Uniti e in Inghilterra, sfruttando l'ampio margine di autonomia di cui godono nella scelta della migliore strategia finalizzata alla prevenzione del rischio, hanno scelto di avvalersi dei nuovi paradigmi tecnologici nella predisposizione di misure organizzative orientate in tal senso[28] o si sono dimostrare propense ad adeguare le stesse attraverso l'utilizzo delle nuove tecnologie[29].

---

[23] In relazione ai connotati propri degli algoritmi di IA da considerarsi generatori di rischi si rimanda al capitolo III del presente contributo

[24] Per un approfondimento sul punto si rimanda al capitolo 1 del presene contributo

[25] V. SEVERINO, *Intelligenza artificiale e diritto penale*, in RUFFOLO (a cura di), *Intelligenza artificiale: il diritto, i diritti, l'etica*, 2020, 537.

[26] Per un'approfondita analisi degli stessi v. SABIA, *Artificial intelligence and environmental criminal compliance*, cit., 187 ss.

[27] In argomento v., MONGILLO, *Presente e futuro della compliance penale*, in *Sist. pen*., 2022, 1 s.

[28] Antesignana del fenomeno della digitalizzazione delle operazioni interne di *compliance* è la Goldman Sachs, società leader a livello mondiale nel settore dell*'investment banking* che dal 1980 ha investito ingenti risorse per la creazione di tecnologie inidonee ad intercettare il rischio, sul punto v. ECONOMIST, *On Top of the World: Goldman Sachs and the culture of risk*, 2006, 11; Alla luce del report condotto da PWC nell'aprile del 2019, *Re-inventing internal controls in the digital age*, molte organizzazioni hanno già adottato e implementato negli anni l'utilizzo di tecnologie emergenti da impiegare nei compiti o processi di controllo, ad esempio l'intelligenza artificiale per il rilevamento delle anomalie o la tecnologia dei droni per portare a termine ispezioni e sorveglianza aerea. *https://www.pwc.com/sg/en/publications/reinventing-internal-controls-in-the-digital-age.html*

[29] Secondo il report "*Integrity in the Spotlight. The future of compliance*", *15th Global Fraud Survey*, stilato da EY nel 2018, il novantuno percento delle imprese intervistate ha dichiarato che la propria organizzazione entro i prossimi due anni adotterà regolarmente sistemi basati sulle tecnologie avanzate, come pagamenti digitali, *Internet of Things* (IoT), robotica e intelligenza artificiale per

La suddetta scelta deriva dalla costatazione di una generale inadeguatezza propria dei sistemi di *compliance* interamente analogici[30]. Questi ultimi, infatti, si dimostrano il più delle volte incapaci di adattarsi alla complessità esterna in cui opera l'impresa e risultano scarsamente efficaci nel predisporre modelli organizzativi idonei a prevenire i reati[31]. È proprio per sopperire alle suddette lacune che si è prospettato il ricorso alle tecnologie, le quali, in virtù delle loro inedite caratteristiche, promettono di porre rimedio alle carenze umane, offrendo in questo modo notevoli opportunità[32] che molte imprese hanno considerato meritevoli di essere sfruttate.

Per comprendere a pieno le potenzialità connesse all'adozione di una *digital criminal compliance* in luogo di quella analogica e le ragioni che giustificano la scelta innovativa operata da molteplici *corporations* anglosassoni, è utile fornire un'analisi delle circostanze fattuali che le imprese si trovano a fronteggiare nella predisposizione dei modelli organizzativi, delineare i profili di inadeguatezza degli strumenti di compliance "classici" ed illustrare in che modo i nuovi presidi tecnologici possano garantire migliori risultati rispetto alle tradizionali metodologie di *compliance.*

Al giorno d'oggi è con un ambiente sempre più improntato alla complessità che gran parte delle *corporations* sono costrette ad interfacciarsi [33]. Una complessità che si estrinseca in una duplice dimensione[34]: quella esterna, ad indicare la pluralità di soggetti, variabili e requisiti normativi che caratterizzano il contesto nel quale l'impresa esercita il suo *business* nonché la dinamicità con cui variano gli stessi variano nel

prevenire il reato di fronde e corruzione *https://www.ey.com/en_be/assurance/how-to-drive-the-future-of-compliance-with-integrity-in-the-spotlight.*

[30] V. SABIA, *Artificial intelligence and environmental criminal Compliance,* cit., 183.

[31] Sul punto v. SCHEMMEL-DIETZEN, *"Effective Corporate Governance" by Legal Tech & Digital Compliance*, in BREIDENBACH, GLATZ, *Rechtshandbuch Legal Tech*, Monaco di Baviera, 2018, 143.

[32] In questi termini BURCHARD, *Digital criminal compliance*, in ENGELHARTKUDLICH, VOGEL (a cura di), *Digitalisierung, Globalisierung und Risikoprävention. Festschrift für Ulrich Sieber zum 70. Geburtstag*, Berlino, 2021, 745.

[33] Sul punto v. SCHEMMEL-DIETZEN, *"Effective Corporate Governance",* 2018, cit. 143.

[34] In argomento v. BAZZERLA, *La gestione della complessità e il controllo di gestione in azienda*, in *Metodi e strumenti controllo di gestione*, 2018, 15 ss.

tempo, e quella interna, in relazione all'articolata struttura organizzativa che l'impresa è tenuta ad adottare per essere competitiva sul mercato e per ridimensionare il rischio di commissione di reati al suo interno.

La complessità nella sua duplice accezione implica un proliferarsi costante di nuovi rischi da prevedere e gestire attraverso un efficace sistema di controllo interno e un costante aggiornamento dell'impianto organizzativo dell'ente. Alla luce di quanto delineato, la prassi dimostra che le tradizionali metodologie impiegate per la prevenzione e gestione del rischio non risultano più in grando di tenere il passo con la mutevole ed articolata realtà circostante e con la conseguente rapida evoluzione dei livelli di rischio[35]. È con l'obiettivo di migliorare i risultati in materia che è stato prospettato l'impiego dei *tools* intelligenti a supporto delle attività di *compliance* e di controllo interno, considerati gli unici paradigmi idonei a gestire i diversi profili di complessità[36].

Un primo elemento fattuale con cui le imprese devono confrontarsi è rappresentato dall'ingente quantità di dati ed informazioni che devono essere processate in tutte le fasi di progettazione di un modello organizzativo[37]. Tali attività di raccolta ed analisi, alla luce delle caratteristiche peculiari che connotano i *big data*[38], non possono essere efficacemente condotte avvalendosi delle tradizionali metodologie di *compliance* che si basano sul solo contributo umano. Ne deriva la constatazione di una generale inadeguatezza dei suddetti sistemi analogici nello sfruttare le importanti potenzialità proprie dei dati e la conseguente necessità di prevedere nuove modalità capaci di conseguire risultati più soddisfacenti[39].

---

[35] Sul punto v. BAMBERGER, *Tecnologies of compliance: risk and regulation in a digital age*, in *Texas law review*, 2010, 285; SABIA, *Artificial intelligence and environmental criminal Compliance*, cit., 184.

[36] V. SABIA, *Artificial intelligence and environmental criminal Compliance,* cit., 183.

[37] BIRRITTERI, *Big Data Analytics e compliance anticorruzione*, in Riv. Trim. Dir. Pen. Cont, 2019, 290; SABIA, *Artificial intelligence and environmental criminal Compliance,* cit., 184;

[38] Per un approfondimento a riguardo si rimanda al primo capitolo del presente contributo

[39] Sul punto v. SCHEMMEL-DIETZEN, "*Effective Corporate Governance",* 2018, cit., 143; BIRRITTERI, *Big Data Analytics e compliance anticorruzione. Profli problematici delle attuali prassi applicative e scenari futuri,* in Riv. Trim. Dir. Pen. Cont., 2019, 289; SABIA, *Artificial intelligence and environmental criminal Compliance,* cit., 184 s.

È in questa direzione che appare utile fare ricorso all'intelligenza artificiale, in modo particolare alla *Big Data Analysis* in tutte le sue declinazioni[40]. Queste tecniche sono dotate di capacità computazionali così sofisticate da risultare idonee ad acquisire, analizzare e mettere in relazione enormi quantità di *data* in maniera completa, veloce ed efficace[41], riuscendo a cogliere dal semplice dato grezzo un profilo di rischio penale che la persona giuridica ha la possibilità di sfruttare nella predisposizione di un modello organizzativo idoneo a prevenire i rischi di commissione dei reati.

È proprio nella capacità di potenziare l'attitudine preventiva dei presidi organizzativi da rintracciare la massima opportunità connessa all'utilizzo della *digital criminal compliance*. Gli algoritmi di IA appaiono infatti idonei a dare concreta attuazione all'finalità più ambiziosa contemplata dal d.lgs 231/2001, vale a dire quella della prevenzione del rischio-reato attraverso la costruzione di un impianto organizzativo così solido da poter essere eluso soltanto attraverso il ricorso a condotte fraudolente[42].

Oltre a costituire un valido supporto nelle diverse fasi di predisposizione dei modelli organizzativi[43], i benefici connessi all'utilizzo della *Big data analysis* sono altresì apprezzabili nelle attività di controllo circa l'adozione, l'attuazione e il corretto funzionamento di questi ultimi. L'impiego di tecniche di analisi altamente sofisticate su grandi volumi di dati, pertanto, in virtù della loro capacità di rilevare anomalie e operare controlli sistematici ed in tempo reale, può costituire un valido supporto per l'ODV[44] che rappresenta l'organismo preposto alle suddette attività.

Un' ulteriore circostanza con cui l'ente deve confrontarsi è rappresentata dall'onerosità della *compliance* tradizionale. La persona giuridica che intende predisporre un MOG idoneo nonché un efficiente sistema di controllo interno si trova, infatti, costretta a sostenere ingenti

[40] Per una trattazione più ampia sul tema si rimanda al primo capitolo del presente contributo
[41] RUSSO, *I modelli di organizzazione, gestione e controllo. Letteratura, prassi e innovazioni tecnologiche*, Milano, 2022, 93 ss; GULLO, *Compliance*, in *Archivio penale*, 2023, 14.
[42] Di questa opinione BIRRITTERI, *Big Data Analytics e compliance anticorruzione*, cit., 295.
[43] Un approfondimento sul punto verrà effettuato nei paragrafi successivi
[44] Anche questo profilo sarà meritevole di un approfondimento ulteriore nei paragrafi successivi

costi[45]. Le principali fonti di aumento delle spese di *compliance* sono due: in primo luogo, la retribuzione dei soggetti coinvolti a vario titolo nelle operazioni di prevenzione del rischio reato[46], in secondo luogo, la complessa articolazione che connota le diverse fasi di predisposizione di un MOG, idonea a mobilitare un ingente quantitativo di risorse.

È nell'abbattimento dei costi di *compliance* che si rinviene un ulteriore punto di forza della digitalizzazione della stessa[47], opportunità rilevante specialmente in un momento in cui le risorse destinate alla prevenzione dei reati nel tessuto aziendale tendono ad essere sempre più limitate.

Quanto alla prima fonte di costi, delegando sempre più compiti ai *tools* intelligenti si andrà a coinvolgere un numero sempre inferiore di persone fisiche, garantendo così all'ente un risparmio di spesa. In aggiunta, l'impiego dei *software* di intelligenza artificiale a supporto delle persone fisiche consentirebbe a queste ultime di risparmiare innumerevoli ore di tempo nel compimento di attività che la macchina, a differenza dell'uomo, è in grado di realizzare in essere in pochi istanti. Quantitativo di tempo ed energie che potrebbe essere meglio impiegato in attività più strategiche e creatrici di valore[48].

In relazione al secondo fattore di spesa, lo sviluppo di sistemi tecnologici consentirebbe alle imprese di semplificare le diverse procedure

---

[45] Sul punto v. BAMBERGER, *Tecnologies of compliance: risk and regulation in a digital age*, in *Texas law review*, cit., 686; CORBELLA, POZZA, *"Modello 231" e "Sistema di controllo interno": aree di sovrepposizione e profili di differenziazione. Implicazioni in termini di costi e benefici sugli assetti degli organi di controllo e vigilanza*, in CENTONZE, MANTOVANI (a cura di), *La responsabilità "penale" degli enti Dieci proposte di riforma*, Bologna, 2016, 60; EY, *Integrity in the spotlight, the future of compliance, 15th Global Fraud Survey*, 2018, 10. *https://www.ey.com/en_gl/assurance/how-to-drive-the-future-of-compliance-with-integrity-in-the-spotlight*; PWC, *Il Modello 231/01 tra innovazioni normative e tecnologiche*, 2019 cit., 8; NISCO, *Riflessi della compliance digitale in ambito 231*, in *Sist. pen*., 2022, 7

[46] A partire dalla fase di costruzione dello stesso fino ai momenti della vigilanza sul suo funzionamento e di aggiornamento.

[47] v. BAMBERGER, *Tecnologies of compliance: risk and regulation in a digital age*, in *Texas law review*, cit., 686; EY, *Integrity in the spotlight, the future of compliance, 15th Global Fraud Survey*, 2018, 10. *https://www.ey.com/en_gl/assurance/how-to-drive-the-future-of-compliance-with-integrity-in-the-spotlight*; PWC, *Il Modello 231/01 tra innovazioni normative e tecnologiche*, 2019 cit., 8; NISCO, *Riflessi della compliance digitale in ambito 231*, in *Sist. pen*., 2022, 7

[48] Cfr., in particolare, il rapporto pubblicato da Deloitte dal titolo: Compliance modernization is no longer optional. How evolved is your approach?, 2017, 5.

di *compliance*, riconducendo, a titolo esemplificativo, l'attività di analisi dei *big data* ad un unico momento piuttosto che a innumerevoli adempimenti posti in essere dalle persone fisiche o, ancora, automatizzando le attività ripetitive basate su regole *standard*. Ne deriverebbe un incremento in termini di efficienza del MOG[49] e una conseguente riduzione dei costi.

Una riduzione dei costi nelle attività in ambito di compliance potrebbe risultare utile ad indurre un maggior numero di imprese a dotarsi di modelli organizzativi volti a prevenire la commissione dei reati nel tessuto dell'impresa. Dando uno sguardo alla situazione italiana, infatti, si assiste ad un'adozione di presidi organizzativi contemplati dal d.lgs. 231/2001 in maniera disomogenea sul territorio nazionale[50]. Le indagini statistiche in merito alla diffusione dei modelli organizzativi testimoniano che sono le imprese di grandi dimensioni i principali interlocutori del decreto mentre quelle di dimensioni più contenute appaiono restie ad organizzarsi in ottica preventiva, prediligendo l'adozione dei modelli solo in un momento successivo alla verificazione della fattispecie criminosa al fine di conseguire i benefici premiali contemplati dal decreto[51].

Un ulteriore elemento fattuale da prendere in considerazione attiene all'ingente quantitativo di nome e *best practices* che le persone giuridiche hanno l'onere di implementare[52]. Anche in questo ambito, se i sistemi di *compliance* "manuali" manifestano profili di inadeguatezza e non riescono a stare al passo con il proliferarsi delle stesse, i nuovi paradigmi tecnologici offrono notevoli opportunità in termini di *compliance* con la regolamentazione.

---

[49] V. BAMBERGER, *Technologies of compliance: risk and regulation in a digital age*, in *Texas law review*, cit., 686

[50] Una prima indagine in materia di diffusione del modello organizzativo è stata condotta nel 2008 a cura di Assonime ed ha registrato la sussistenza di un MOG nel 73% delle imprese intervistate, con la precisazione che solo 131 delle 300 società sentite erano di piccole o medie dimensioni, sul punto v. Indagine sull'attuazione del decreto legislativo 231/2001, a cura di Assonime, maggio 2008, reperibile su *www.assonime.it*
Una seconda rilevazione in materia è stata curata da Tim e Confindustria nel 2017. Quest'ultima dimostra la scarsa diffusione del modello organizzativo tra le PMI in quanto solo 16 dei 45 enti intervistati, vale a dire il 36% del totale, ha confermato di essersi organizzata in chiave preventiva. Sul punto v. Indagine modelli organizzativi 231 e anticorruzione, a cura Confindustria e Tim, aprile 2017.

[51] Cfr. MANACORDA*, L'idoneità preventiva dei modelli di organizzazione*, cit., 63.

[52] V. SABIA, *Artificial intelligence and environmental criminal Compliance,* cit., 183.

Una prima ragione che fa propendere per l'adozione della *digital criminal compliance* riguarda l'opportunità di incorporare i requisiti normativi in un sistema informatico con l'obiettivo di garantire il rispetto di questi ultimi ed abbattere il rischio di elusione degli stessi[53]. Un'ulteriore potenzialità derivante dall'impiego dei *tools* attiene alla loro capacità di rilevare e recepire tutte le innovazioni verificatesi nel contesto normativo di riferimento attraverso l'impiego di tecniche di *data analysis*, garantendo pertanto all'ente la possibilità di essere *compliant* con tutti gli aggiornamenti normativi entrati in vigore[54] e di ridurre il rischio di incorrere in sanzioni.

Un quarto elemento con cui le nuove *corporations* devono interfacciarsi riguarda il recente inserimento dei reati informatici nel novero dei reati c.d. presupposto espressamente contemplati negli articoli 24 e seguenti del d.lgs. 231/2001. Si tratta di fattispecie criminose poste in essere il più delle volte da soggetti esperti di tecnologia che si avvalgono di strumenti informatici o dell'informazione per arrecare danno a diversi beni giuridici tutelati dal nostro ordinamento[55].

Per via delle metodologie impiegate dalle persone attive e dell'ambito in cui il più delle volte si realizzano i reati in questione[56], l'impiego dei presidi classici di *compliance* appare inadeguato a prevenire e a contrastare gli stessi. È anche in questo frangente che l'utilizzo delle tecnologie di IA potrebbe rappresentare una valida soluzione, garantendo all'ente di competere "ad armi pari" con i criminali esperti di informatica.

È alla luce di quanto delineato finora che si giustifica la scelta delle *corporations* con sede nei paesi anglosassoni di sfruttare le opportunità derivanti dall'utilizzo delle nuove tecnologie a supporto della *compliance*, in modo particolare per prevenire e gestire il rischio-corruzione[57].

---

[53] Sul punto v. MORGANTE, FIORINELLI, *Promesse e rischi della compliance penale digitalizzata*, cit., 7.

[54] Cft. QUEST, CHARRIE, DU CROO DE JONGH, ROY, *The risks and benefits of using AI to detect a crime*, in *Harvard Business Review*, 2018, 3; PWC, *Il Modello 231/01 tra innovazioni normative e tecnologiche*, 2019 cit., 8

[55] Cfr. GULLO, *I reati informatici*, in LATTANZI, SEVERINO (a cura di*), Responsabiità da reat*o, vol. I, Torino, 2021, 384 ss.

[56] Si fa riferimento al *web*

[57] Per un approfondimento sul punto v. BIRRITTERI, *Big Data Analytics e compliance anticorruzione*, 2019, cit., 290.

Appare opportuno precisare che le strategie organizzative messe in campo dalle imprese private non delegano per intero l'attività di predisposizione di un modello organizzativo ad un *software*, posto che gli sviluppi tecnologici attuali consentono di progettare sistemi di intelligenza artificiale nell'accezione debole del termine, pertanto ancora bisognosi del contributo dell'uomo. L'intelligenza artificiale nell'ambito della *criminal compliance* viene quindi a porsi come un *empowerment organzzativo*, vale a dire un fattore di miglioramento della capacità organizzativa della persona giuridica attraverso l'istaurazione di una sinergia tra intelligenze: quella umana e quella artificiale.

2. Impiego delle nuove tecnologie nella creazione di un modello organizzativo idoneo alla luce delle indicazioni fornite dal d.lgs. 231/2001

Una volta prospettate le opportunità derivanti dall'impiego dei nuovi paradigmi tecnologici alla *criminal compliance*, è utile soffermarsi sulla nozione di modello organizzativo ed illustrarne gli elementi costitutivi per poi comprendere quali tecnologie nello specifico possano essere impiegate nella costruzione dello stesso così da concretizzare quanto delineato poc'anzi a livello teorico.

Il modello organizzativo (MOG) contemplato dal d.lgs. 231/2001 rappresenta «l'architrave»[58] del sistema di responsabilità degli enti, la centralità dello stesso nell'impianto normativo delineato dal decreto si spiega per tre ordini di motivi.

In primo luogo, lo stesso rappresenta la concretizzazione della *compliance* penale, «filosofia»[59] che permea tutte le scelte operate dal legislatore del 2001[60]. Il modello organizzativo si traduce, infatti,

[58] In questi termini GULLO, *I modelli organizzativi*, in LATTANZI, SEVERINO (a cura di), *Responsabilità da reato*, cit., 385.
[59] Così MONGILLO, *Presente e futuro della compliance penale*, in *Sist. pen*., 2022, 3.
[60] Autorevole dottrina si riferisce al modello organizzativo quale "supporto materiale del dovere organizzativo dell'ente", così MONGILLO, *Il giudizio di idoneità del Modello di organizzazione ex d.lgs. 231/2001: incertezza dei parametri di riferimento e prospettive di soluzione*, in *La resp. Amm. delle società e degli enti*, 2011, 3, 70, il quale richiama la stessa definizione fornita da PIERGALLINI,

nell'insieme di regole di condotta orientate a contenere il rischio[61] che i soggetti operanti a vario tiolo nell'impresa propendano a livello etico e siano materialmente capaci di integrare una delle fattispecie criminose contemplate dal d.lgs. 231/2001[62].

È, pertanto, nella prevenzione del rischio-reato da rintracciare l'obiettivo più ambizioso che l'ente intende perseguire mediante la predisposizione di misure organizzative concrete, un onere ricompensato dal legislatore del 2001 con la possibilità per la persona giuridica di ottenere una serie di benefici sul piano penalistico qualora i suddetti presidi vengano adottati, efficacemente attuati nonché considerati idonei a prevenire i reati tassativamente enumerati nel decreto[63].

Il secondo profilo che attesta la centralità del modello è rappresentato proprio dagli elementi di premialità che l'ente ha la possibilità di conseguire in virtù della predisposizione di un modello organizzativo valutato dall'autorità giudiziaria come idoneo. Secondo la logica delineata dal decreto 231, il modello diviene il «bastone» di cui serve il legislatore per consentire all'ente di conquistare la «carota»[64], rappresentata dall'esonero totale o parziale della responsabilità nonché dall'esclusione o attenuazione della risposta sanzionatoria, all'interno di una più generale

---

i modelli organizzativi, in AA. VV., LATTANZI (a cura di), Reati e responsabilità degli enti. Guida al d.lgs. 8 giugno 2001, n. 231, 157.

[61] Si parla di contenimento del rischio e non di eliminazione dello stesso in quanto la prospettiva "rischio-zero" rappresenta una chimera, a maggior ragione se il rischio da governare si sostanzia in condotte illecite, sul punto v. MONGILLO, *Presente e futuro*, 2022, cit., 3; ALESSANDRI, *Diritto penale e attività economiche*, Bologna, 2010, 225.

[62] Definizione contenuta in CORBELLA, POZZA, *«Modello 231» e «Sistema di controllo interno»: aree di sovrapposizione e profili di differenziazione. Implicazioni in termini di costi e benefici sull'assetto degli organi di controllo e vigilanza*, in CENTONZE, MANTOVANI (a cura di), *La responsabilità "penale" degli enti, dieci proposte di riforma*, Bologna, 2016, 53 s.

[63] Sul punto v. MANACORDA, *L'idoneita` preventiva dei modelli di organizzazione nella responsabilita`da reato degli enti: analisi critica e linee evolutive*, in *Riv. trim. dir. pen. econ*, 2017, 52 s.

[64] Si fa riferimento allo "*stick and carrot approch*", teoria di derivazione anglosassone in quanto prospettata per la prima volta dal filosofo Jeremy Bentham nel corso della prima rivoluzione industriale. La logica Si tratta di un sistema in virtù del quale si è premiati in conseguenza a determinati comportamenti e si è puntiti a seguito di altri, secondo la definizione fornita dal Cambridge dictionary. Sul punto v. DE MAGLIE, *L'etica e il mercato. La responsabilità penale delle società*, Milano, 2002,73 ss.

considerazione dell'ente quale soggetto razionale e quindi orientato a massimizzare i benefici con la contestuale riduzione dei costi[65].

L'adozione e l'attuazione del MOG rappresentano quindi il "prezzo" da pagare per l'ente in cambio di una serie di benefici che seguono una «logica scalare» in quanto sono di maggiore o minore entità a seconda del momento in cui il modello viene adottato[66].

È in questa prospettiva che viene in rilievo la differenziazione tra modello c.d. *ante delictum* e modello c.d. *post factum*[67]. La prima declinazione di MOG è disciplinata dagli artt. 6 e 7 del decreto e, come si evince dalla denominazione, implica l'adozione del modello in un momento cronologicamente anteriore alla commissione della fattispecie criminosa ascritta all'ente. Quest'ultima rappresenta la tipologia di modello principale in quanto consente alla persona giuridica di ottenere il beneficio più ambizioso, vale a dire l'esonero totale da responsabilità *ex criminis*.

Tale risultato è conseguibile qualora l'ente abbia, in primo luogo, adottato ed efficacemente attuato un modello organizzativo idoneo ed abbia, in secondo luogo, affidato ad un organismo interno dotato di autonomi poteri di iniziativa e controllo sia il compito di vigilare sul funzionamento e l'osservanza del MOG che la responsabilità di curare il loro aggiornamento.

Entrambi gli adempimenti devono essere portati a termine sia nel caso in cui il reato sia stato commesso da un soggetto che riveste una posizione subordinata nell'organico dell'ente, che nell'eventualità in cui a porre in essere la fattispecie criminosa sia stata una persona fisica nel ruolo di apicale, con la differenza che in questo secondo caso si richiede altresì la prova dell'elusione fraudolenta del modello da parte dei vertici[68].

La seconda tipologia di MOG contemplata dal decreto legislativo prende il nome di modello *post factum* e fa riferimento all'insieme

---

[65] Così PATERNOSTER, SIMPSON, *A Rationale Choice Theory in Corporate Crime*, in CLARKE, FELSON (a cura di), *Routine Activity and Rational Choice*, vol. 5, Londra, 1993, 37 ss.

[66] Cfr. FORTI, *Il crimine dei colletti bianchi come dislocazione dei confini normativi. "Doppio standard" e "doppio vincolo" nella decisione di delinquere o di blow the whistle*, in ALESSANDRI, ALBERTO (a cura di), *Impresa e giustizia penale: tra passato e futuro. Atti del convegno (Milano, 14-15 marzo 2022)*, Milano, 2009, 223 ss.

[67] In argomento v. MANACORDA, *L'idoneità preventiva dei modelli di organizzazione*, cit., 62 ss.

[68] Ex. art 6, co. 1, lett. c, d.lgs 231/2001

«strumenti di ravvedimento»[69] che la persona giuridica decide di predisporre in un momento successivo alla verificazione dell'illecito. Anche in relazione a questa seconda ipotesi, il decreto 231 contempla una serie di benefici per l'ente che sia organizzato seppur in maniera tardiva, nell'ottica di indurre lo stesso a ricollocarsi nei binari della legalità. Quest'ultimo obiettivo, insieme a quello più ambizioso della prevenzione del rischio-reato, rappresenta una delle principali finalità che il legislatore del 2001 ha inteso perseguire[70].

Le differenze che intercorrono tra il MOG *ante delictum* e il MOG *post factum* sono principalmente due e attengono al momento in cui la persona giuridica si adopera nel predisporre i presidi organizzativi, successivamente alla commissione del reato presupposto in questo secondo caso, e all'entità dei benefici volti a premiare l'organizzazione, logicamente minori in relazione a quest'ultima tipologia di modello[71].

A seconda sia del preciso momento in cui l'impresa decide di attuare le condotte riparatorie che delle specifiche circostanze contemplate dagli articoli di riferimento, il decreto legislativo stabilisce benefici diversi in favore della persona giuridica, la cui entità risulta inversamente proporzionale al periodo di ritardo maturato con l'obiettivo di incentivare l'ente ad adoperarsi quanto prima[72].

Se l'adozione e l'efficace attuazione intervengono in un momento precedente alla dichiarazione di apertura del dibattimento di primo grado, ne consegue una riduzione della sanzione pecuniaria da un terzo alla metà, a patto che l'ente abbia risarcito integralmente il danno e abbia eliminato le conseguenze dannose o pericolose del reato ovvero si sia comunque

[69] Sul punto v. VARRASO, *Il procedimento per gli illeciti amministrativi dipendenti da reato*, Milano, 2012, 92.
[70] Cfr. RUGGIERO, *Scelte discrezionali del pubblico ministero e ruolo dei modelli organizzativi nell'azione contro gli enti*, Torino, 43 ss.
[71] si esclude l'esonero da responsabilità ma si dà la possibilità all'ente di fruire di vantaggi sul piano sanzionatorio.
[72] Al legislatore del 2001, più che punire l'ente in conseguenza delle condotte criminosa poste in essere, è interessato incentivare lo stesso a organizzarsi ex ante per prevenire il compimento di un reato o ritornare nei parametri della legalità attraverso l'adozione di condotte riparative indurre lo stesso a riorganizzarsi

efficacemente adoperato in tal senso[73]. È della metà la riduzione della pena nel caso in cui il fatto sia stato commesso dall'apicale o dal sottoposto nel prevalente interesse proprio o di terzi qualora l'ente non ne abbia ricavato vantaggio alcuno o soltanto minimo, in aggiunta alla circostanza che il danno patrimoniale cagionato sia di particolare tenuità[74]. Infine, in presenza di tutte le condizioni finora esplicitate, l'ente avrà la possibilità di scontare una pena ridotta dalla metà ai due terzi[75].

Se l'articolo 12 del decreto in esame si concentra esclusivamente sulle sanzioni pecuniarie, l'articolo 17 testimonia l'ulteriore volontà del legislatore di rinunciare all'applicazione delle più gravose sanzioni interdittive al ricorrere delle condizioni poc'anzi menzionate, contestualmente alla eliminazione da parte dell'ente delle carenze organizzative che hanno determinato il reato attraverso l'adozione e l'attuazione di modelli organizzativi idonei a prevenire reati della specie di quello verificatosi[76].

L'adozione e l'efficace attuazione di un modello organizzativo *post factum* è consentita anche in un arco temporale ancora successivo, vale a dire dopo la dichiarazione di apertura del procedimento di primo grado. Si prevede la possibilità per l'ente che abbia adempiuto alle circostanze contemplate dall'art 17 di richiedere la conversione delle sanzioni interdittive in sanzioni pecuniarie, connotate da un tasso di afflittività inferiore[77]. Tale richiesta deve essere presentata nel termine massimo di venti giorni dalla notifica dell'estratto della sentenza di condanna e abilita il giudice dell'esecuzione a decidere in merito alla conversione, determinandone l'importo «in una somma non inferiore a quella già

[73] Ai sensi dell'art 12 co 2 d.lgs 231/2001, per un commento v. GULLO, *I modelli organizzativi*, in LATTANZI, SEVERINO (a cura di), cit., 242.
[74] Ex art 12 co 1 d.lgs 231/2001
[75] Ex art 12 co. 3 d,lgs 231/2001 sul punto v. MONGILLO, BELLACOSA, *Il sistema sanzionatorio*, in LATTANZI, SEVERINO (a cura di), *Responsabiità da reato degli enti*, vol. I, Torino, 2020, 302 ss.
[76] Ai sensi dell'art. 17 co. 1 lett. b d.lgs 231/2001
[77] V. MONGILLO, BELLACOSA, *Il sistema sanzionatorio*, in LATTANZI, SEVERINO (a cura di), *Responsabiità da reato*, 2020, cit., 304

applicata in sentenza e non superiore al doppio della stessa» in caso affermativo[78].

Se le imprese di grandi dimensioni propendono sistematicamente per l'adozione di un modello *ante delictum*, nonostante nella prassi giudiziaria siano estremamente rare le pronunce volte a riconoscere l'idoneità del MOG e a concedere l'esonero della responsabilità quale conseguenza dello stesso[79], gli enti di piccole e medie dimensioni, anche in virtù di questa circostanza, tendono ad investire in termini di *compliance* e ad adottare misure riparative solo nell'eventualità in cui venga istaurato un procedimento penale nei loro confronti e quindi solo in un momento successivo alla verificazione della fattispecie criminosa nel tessuto aziendale[80].

Sia la tendenza propria dei tribunali italiani a disconoscere l'idoneità di un modello organizzativo che la scarsa adozione in ottica preventiva dello stesso da parte delle PMI[81], dimostrano la scarsa efficacia dell'approccio delineato dal decreto ma soprattutto del processo di valutazione giudiziaria dei modelli, spesso tendente a presumere l'inidoneità degli stessi per il solo fatto che si sia verificata una fattispecie criminosa, senza scendere nel merito.

Una testimonianza delle difficoltà incontrate dalla magistratura nel delineare dei criteri oggettivi su cui basare il giudizio di idoneità del modello[82] e, al tempo stesso, un'inversione di tendenza rispetto alla presunzione di inidoneità, è rappresentata dalla vicenda Impregilo. La vicenda è stata interessata da ben sei gradi di giudizio che hanno visto la contrapposizione di due approcci principali e antitetici tra loro relativi alla valutazione della condotta tenuta dalla persona giuridica e

[78] Ex art. 78, d.lgs 231/2001
[79] V. GULLO, *I modelli organizzativi*, in LATTANZI, SEVERINO (a cura di), cit., 267 ss.; BIRRITTERI, *Big Data Analytics e compliance anticorruzione*, cit., 298
[80] Cfr, GULLO, *I modelli organizzativi*, in LATTANZI, SEVERINO (a cura di), cit., 247
[81] Le PMI rappresentano il 92% delle aziende attive sul territorio italiano, dato illustrato da Il sole 24 ore nel 2019, *https: //www.infodata.ilsole24ore.com/2019/07/10/40229*
[82] V. COLACURCI, *L'idoneità del modello nel sistema 231, tra difficoltà operative e possibili correttivi*, in *Dir. Pen. Cont*., 2016, 68.

all'interpretazione da conferire al parametro dell'«elusione fraudolenta» contemplato dall'art 6 d. lgs 231 del 2001.

Se i giudici di merito hanno riconosciuto l'idoneità del modello a prevenire il reato di aggiotaggio con diffusione di notizie false nella versione vigente all'epoca[83], con conseguente assoluzione dell'ente quanto al reato di specie[84], i giudici di legittimità, alla prima occasione in cui sono stati chiamati a pronunciarsi, hanno ribaltato le argomentazioni addotte in primo grado e confermate nel secondo, annullando con rinvio la sentenza di appello e riconoscendo l'inadeguatezza del modello con conseguente ascrizione della responsabilità in capo alla persona giuridica. Successivamente, il giudice del rinvio ha confermato l'assoluzione dell'ente rafforzando le argomentazioni già sostenute in precedenza in una sentenza che è stata ulteriormente oggetto di impugnazione da parte della Procura generale. In questa seconda occasione di pronuncia, la Corte di legittimità ha riconfermato l'innocenza della persona giuridica alla luce di alcune osservazioni meritevoli di un approfondimento ulteriore.

Il reato verificatosi nella vicenda Impregilo aveva ad oggetto la diffusione di informazioni *price sensitive* false con l'obiettivo di alterare la valutazione degli strumenti finanziari sul mercato[85]. Nel caso di specie, si rimproverava all'ente di essersi avvantaggiato della suddetta condotta criminosa in quanto la stessa avrebbe provocato una notevole alterazione del valore delle azioni societarie e delle obbligazioni emesse da società del gruppo.

Per prevenire la verificazione della suddetta fattispecie criminosa, l'ente aveva elaborato uno specifico protocollo per la formazione delle comunicazioni verso l'esterno che si estrinsecava in tre passaggi principali:

---

[83] Il reato di aggiotaggio era previsto quale reato presupposto ai sensi dell'articolo 25-ter d.lgs. 231/2001

[84] Si tratta della prima pronuncia dall'entrata in vigore del d.lgs. 231/2001 ad attestare l'idoneità del modello organizzativo adottato dalla persona giuridica con conseguente assoluzione della stessa.

[85] Il delitto di aggiotaggio, all'art. 2637 c.c., prevede : «chiunque diffonde notizie false, ovvero pone in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, ovvero ad incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o di gruppi bancari , è punito con la pena della reclusione da uno a cinque anni».

la predisposizione delle comunicazioni in un documento da parte dei funzionari aziendali competenti, la formazione di una bozza di comunicato stampa a cura delle relazioni esterne e l'approvazione finale della stessa da parte di Presidente e Amministratore delegato. In aggiunta, era stato previsto che un OdV fosse deputato alla vigilanza della sopra indicata procedura e alla segnalazione di eventuali irregolarità[86].

Secondo la magistratura di primo grado, i suddetti presidi organizzativi sarebbero stati idonei a prevenire in reato di aggiotaggio, nonostante lo stesso si fosse poi verificato materialmente.

I giudici di merito argomentano affermando che andrebbe esclusa una presunzione di inidoneità per dare spazio ad un giudizio di «prognosi postuma» utile a verificare in concreto l'adeguatezza dei presidi organizzativi implementati[87] e attestano altresì che l'adozione di modello organizzativo da parte dell'ente subito dopo l'entrata in vigore del decreto, «con una tempestività quasi senza precedenti»[88] nonostante non vi fossero precedenti in materia[89], testimonia l'intenzione dello stesso di mantenersi nei binari della legalità.

In aggiunta, viene riconosciuta la natura fraudolenta della condotta posta in essere dai vertici dell'ente in quanto non direttamente riconducibile ad un *deficit* organizzativo proprio della persona giuridica ma derivante dalla violazione delle regole interne previste da quest'ultima[90]. Gli apicali, infatti, non tenendo conto delle valutazioni ad opera dei funzionari della società, avrebbero forzato la procedura e scelto, con ampi margini di

[86] In argomento v. PALIERO, *Responsabilità dell'ente e cause di esclusione della colpevolezza: decisione lassista o interpretazione costituzionalmente orientata?*, in *Le Società*, 2010, 141.
[87] Cfr. ARENA, *La responsabilità amministrativa delle imprese: il d.lgs. n. 231/2001: Normativa, Modelli organizzativi, temi d'attualità*, in *Nuova Giuridica*, 148.
[88] Cfr. G.U.P. Trib. Milano (Manzi), 17 Novembre 2009, in *Le Società*, n. 4, 2010, 474.
[89] Secondo parte della dottrina, i giudici di primo grado hanno voluto premiare la tempestività con cui l'ente ha deciso di implementare le indicazioni contenute nel decreto 231, v. PALIERO, *Responsabilità dell'ente e cause di esclusione della colpevolezza: decisione «lassista» o interpretazione costituzionalmente orientata?*, commento a sentenza G.U.P. Trib. Milano (Manzi), 17 Novembre 2009, in *Le Società*, 2010, 477
[90] G.U.P. Trib. Milano, 17/11/2009, Impregilo S.p.A., cit., p. 476, il Tribunale, in particolare, statuisce che «se si fosse seguita la procedura prevista dal modello sarebbe stato impossibile per gli imputati attuare il loro proposito di 'rassicurare' il mercato e di "abbellire" il bilancio della società in danno degli investitori».

discrezionalità, il contenuto delle comunicazioni, circostanza che, sommata alle altre sopra menzionate, avrebbe indotto la magistratura ad escludere una responsabilità *ex crimine* in capo alla società.

Già in momento immediatamente successivo alla pubblicazione della sentenza di primo grado, parte della dottrina[91] aveva rilevato come quella considerata dai giudici di merito fosse una «nozione stringata di fraudolenza» in quanto prescindente dalla sussistenza di artifizi e raggiri e basata su un'interpretazione soggettiva del criterio in esame.

Quanto incardinato nella sentenza di primo grado e confermato nel secondo, è stato ribaltato da parte della Corte di Cassazione nel terzo grado di giudizio[92]. I giudici di legittimità hanno alla magistratura di merito in *primis* il fatto di aver condotto un giudizio di idoneità superficiale e non basato sulla concreta attitudine del modello a prevenire il reato verificatosi[93]. Il MOG adottato dalla Impregilo S.p.a. infatti, non contemplava alcun controllo effettivo in merito ai comunicati stampa ad opera dei vertici, consentendo agevolmente agli stessi di modificarli e diffonderli a proprio piacimento, elemento che testimonierebbe la scarsa capacità del presidio di evitare la realizzazione di fattispecie criminose di questo tipo. La Corte osserva infatti che «se all'organo di controllo non fosse nemmeno concesso di esprimere una *dissenting opinion* sul "prodotto finito"[94], è evidente che il modello organizzativo non possa ritenersi atto a impedire la consumazione di un tipico reato di consumazione».

In secondo luogo, nel terzo grado di giudizio si è attestata la mancata sussistenza dell' elemento dell'«elusione fraudolenta», in quanto lo stesso non si estrinseca nella semplice violazione di una regola interna ma richiede un *quid pluris*, una condotta «ingannevole, falsificatrice, obliqua, subdola»

---

[91] Cfr. COLACURCI, *L'idoneità del modello nel sistema 231*, cit., 75

[92]Cfr. Cass., Sez. V, 30/01/2014, Impregilo S.p.A., in *Le Società*, 2014, 469 ss. Per un commento alla sentenza, si veda, tra gli altri, BARTOLOMUCCI, *Ribadita dalla S.C. la centralità dell'art. 6, d.lgs. n. 231/2001 nella valutazione giudiziale della idoneità ed effettività del modello*, in *Resp. amm. soc. ed enti*, 2014, n. 2, 265 ss; PALIERO, SALAFIA, *L'imputazione della responsabilità all'ente per il fatto-reato dei soggetti apicali: il punto di vista della Cassazione*, in *Le Soc.*, 2014, 469.

[93] Cfr. MONTESANO, *Il caso Impregilo: la Cassazione definisce delle regole più rigorose in relazione all'accertamento della efficacia dei modelli organizzativi (Commento a Cass. pen., Sez. V, n. 4677, 30 gennaio 2014)*, in *Rivista 231*, 102.

[94] Così, Cass., Sez. V, 30/01/2014, Impregilo S.p.A., 471.

tale da produrre l'interruzione del rapporto di identificazione tra amministratori ed ente, idoneo ad escludere una responsabilità *ex criminis* in capo a quest'ultimo[95].

L'ultima riflessione contenuta nella sentenza di legittimità riguarda la valenza da dare alle *best practices* elaborate da Confindustria. Secondo la Corte, le stesse non andrebbero considerate quali criteri normativi veri e propri, tanto che la loro osservanza da parte della persona giuridica non varrebbe a riconoscere l'idoneità del modello predisposto e l'esclusione dal *tertium genus* di responsabilità.

A seguito del rinvio in corte d'appello, il 10 dicembre 2014 la Corte territoriale ha confermato la sentenza assolutoria sostenendo, in aggiunta, che l'elemento dell'elusione fraudolenta si sarebbe verificato alla luce di un accordo collusivo tra i vertici dell'ente, volto a diffondere informazioni *price sensitive* erronee ed ingannevoli.

La suddetta pronuncia è stata nuovamente impugnata da parte della Procura generale dinanzi alla Corte di Cassazione e il ricorso si è concluso con l'emanazione della sentenza in data 11 novembre 2021, le cui motivazioni sono state pubblicate nel mese di giugno dell'anno successivo. Quest'ultima ha "messo la parola fine" alla vicenda Impregilo stabilendo in via definitiva che la società in questione non è responsabile di quello che ad oggi è l'illecito amministrativo contemplato dall'articolo 24 ter, lett. r) d.lgs. 231/2001[96].

I giudici di legittimità, in una sentenza "modello", hanno fatto chiarezza in merito alla struttura, all'oggetto e all'illecito dell'ente. In primo luogo, la Corte esclude categoricamente una valutazione dei modelli basata sul *post hoc*, ribadendo che la verificazione di un reato in azienda non decreta l'inadeguatezza del modello, in secondo luogo conferma che per

[95] BARTOLOMUCCI, *L'adeguatezza del Modello nel disposto del d.lgs. 231 e nell'apprezzamento giudiziale. Riflessioni sulla sentenza d'appello "Impregilo"*, in *Resp. amm. soc. ed enti*, 2012, 172.
[96] In argomento v. BORGOBELLO, *Sentenza Impregilo: metodi di valutazione di adeguatezza del modello organizzativo, dei poteri dell'Organismo di vigilanza e della condotta fraudolenta degli amministratori*, in *Giurisprudenza Penale*, 2022; FUSCO, PALIERO, *L'"happy end" di una saga giudiziaria: La colpa di organizzazione trova "forse" il su tipo*, in *Sistema Penale*, 2022, 115. PIERGALLINI, *Una sentenza "modello" della cassazione pone fine all'estenuante vicenda "Impregilo",* in *Sistema penale*, 2022, 1 ss.

riconoscere la sussistenza di una colpa di organizzazione, occorre che la condotta illecita corrisponda proprio a quel pericolo che la regola cautelare intendeva escludere, in ultimo, viene affermato che l'approccio argomentativo basato sulla "prognosi postuma" sia l'unico valido[97].

Nell'affrontare il *vulnus* del MOG concretamente adottato dalla Impregilo Spa, che si sostanza nella presenza di un Organismo di vigilanza scarsamente efficace perché a composizione monocratica e strettamente dipendente dal Presidente del Cda, la Corte si è domandata se fosse opportuno decretare la mancata adeguatezza di un apparato organizzativo alla luce di una sola lacuna, rispondendo negativamente al suddetto interrogativo e giungendo alla conclusione che occorra altresì la sussistenza di un nesso causale tra la falla interna al MOG e la verificazione del reato presupposto.

Quest'ultima sentenza di legittimità statuisce il principio per cui non può essere considerato esigibile un controllo preventivo da parte dell'OdV su tutte le operazioni poste in essere dagli apicali dell'ente, allo stesso spetta infatti il compito di individuare e segnalare eventuali criticità proprie del modello e non porre in essere un vero e proprio controllo gestorio, a maggior ragione con riferimento ai reati di comunicazione[98].

Quanto alla sussistenza dell' elemento dell' elusione fraudolenta da parte degli apicali, la Corte ha affermato che solo una condotta ingannevole, falsificatrice, obliqua e subdola sarebbe stata in grado di disattendere la proceduta a tre fasi predisposta dalla società che, per di più, contemplava la presenza di più soggetti[99].

In ultimo, in relazione al ruolo da dare alle linee guida di settore, la Corte si limita a confermare la precedente impostazione che ha escluso in capo agli stessi il valore di criteri normativi, sostenendo che il rispetto degli stessi non basta ad ottenere un giudizio positivo di adeguatezza

[97] Sul punto v. FUSCO, PALIERO*, L'"happy end" di una saga giudiziaria: La colpa di organizzazione trova "forse" il su tipo*, in *Sistema Penale*, 2022, 124 ss; PIERGALLINI, *Una sentenza "modello" della cassazione pone fine all'estenuante vicenda "impregilo"*, in *Sistema penale*, 2022, 3.
[98] Cfr. PIERGALLINI, *Una sentenza "modello" della cassazione*, cit., 7 s.
[99] V. FUSCO, PALIERO, *L'"happy end" di una saga giudiziaria: La colpa di organizzazione trova "forse" il su tipo*, cit., 132 ss.

dell'apparato organizzativo predisposto. Per contro, si prescrive alla magistratura orientata a disattendere l'idoneità di un MOG nonostante il rispetto da parte dell'ente delle *best practices* di addurre una motivazione rafforzata al suddetto giudizio[100].

Alla luce delle circostanze sopra prospettate e degli approdi a cui si è giunti a seguito della vicenda Impregilo, si auspica un intervento di riforma da parte del legislatore volto a dare concreta attuazione alle finalità alle quali è improntato l'intero decreto 231[101]. Sarebbe opportuna, in tal senso, una definizione più dettagliata delle misure organizzative che una persona giuridica è tenuta ad adottare affinché il modello predisposto dalla stessa venga considerato idoneo, dal momento che i riferimenti giuridici attualmente in vigore risultano scarni e generici[102]. In questo modo, si andrebbe ad incrementare la certezza del diritto, gli ampi margini di discrezionalità in capo all'autorità giudiziaria verrebbero ridimensionati e l'impresa avrebbe maggiori opportunità di godere del beneficio massimo prospettato dal decreto 231, vale a dire l'esonero dal *tertium genus* di responsabilità[103].

Il ruolo di assoluta centralità del MOCG risulta evidente anche nella sistematica dell'illecito in quanto il modello organizzativo viene a configurarsi come «architrave» della responsabilità ascrivibile all'ente[104].

Al fine di scongiurare ogni forma di responsabilità oggettiva con conseguente violazione dell'articolo 27 co 1 che ne fa esplicito divieto e gli

[100] V. PIERGALLINI, *Una sentenza "modello" della cassazione pone fine all'estenuante vicenda "impregilo",* in *Sistema penale*, 2022
, 3.
[101] Si fa riferimento alla prevenzione del rischio-reato e al ravvedimento postumo da parte della persona giuridica
[102] Di questa opinione BIRRITTERI, *Big Data Analytics e compliance anticorruzione*, cit., 298
[103] La natura della responsabilità in capo all'ente introdotta per la prima volta dal decreto 231/2001 è stata oggetto di un fervente dibattito in dottrina. Se autori come, propendono per la natura amministrativa della stessa e studiosi del diritto quali sono dell'idea che quest'ultima sia penale, la relazione ministeriale al decreto e, in ultimo, la sentenza Tyssenkrupp, la considerano un t*ertium genus* di responsabilità in quanto coniuga i tratti essenziali del sistema penale e di quello amministrativo. Sul punto v. PELISSERO, SCAROINA, NAPOLEONI, *Principi generali*, in LATTANZI, SEVERINO (a cura di), *Responsabilità da reato degli enti*, Torino, 2020, 154 ss.
[104] V. GULLO, *I modelli organizzativi*, in LATTANZI, SEVERINO (a cura di), cit., 241.

articoli 6 e 7 della Convenzione europea dei diritti dell'uomo[105], il legislatore del 2001, discostandosi dai paradigmi di responsabilità dell'ente diffusesi nel nord America[106], ha disciplinato negli articoli 6 e 7 del d.lgs 231 del 2001[107] l'elemento soggettivo della c.d. colpa da organizzazione. È una tipologia di colpa a carattere squisitamente normativo che si basa interamente sui modelli organizzativi[108] dal momento che si sostanzia in un *deficit* di organizzazione[109]. Si tratta in concreto del rimprovero da muovere all'ente che non ha predisposto o adottato le cautele organizzative volte a ridurre significativamente il rischio di compimento del reato ovvero che non ha adempiuto i controlli sulle stesse stabiliti nel decreto[110].

Preso atto del ruolo centrale rivestito dal modello organizzativo nel sistema normativo delineato dal d.lgs. 231 del 2001 in rappresenta la concretizzazione della *compliance*, il presupposto dei profili di premialità contemplati nel decreto e il fondamento della colpa di organizzazione, è utile entrare nel merito della sua composizione per poi illustrare il suo funzionamento in concreto.

---

[105] Applicabili nel nostro ordinamento in virtù di quanto disposto dall'art 117 Cost, i quali impongono la sussistenza di una forma di colpevolezza anche a livello convenzionale

[106] Si fa riferimento, in modo particolare, ai modelli di *vicarious liabiity* i quali contemplano una forma di responsabilità oggettiva del *master* per ogni fattispecie criminosa posta in essere da un sottoposto nel contesto aziendale, per approfondimenti sul punto v. SABIA, *Artificial intelligence and environmental criminal compliance*, in DE LA PARRA, GULLO, MAZZACUVA (a cura di), *The Criminal Law Protection* , cit., 185 ss.

[107] Alla luce del testo normativo, la colpa di organizzazione si declina diversamente a seconda che il reato sia stato posto in essere da un soggetto apicale o da un soggetto sottoposto, sul punto v. DI GIOVINE, *Il criterio di imputazione soggettiva*, in LATTANZI, SEVERINO (a cura di), *Responsabilità da reato degli enti*, vol I, diritto sostanziale, Torino, 2020, 205 ss., di fatto però la distinzione ha subito un sostanziale ridimensionamento sia nella prassi interna agli enti, in quanto i modelli adottati sono unitari a prescindere dalla qualifica del soggetto attivo come dimostrato nello studio Assonimme 2008, che in virtù della sentenza ThyssenKrupp, che ha definitivamente chiarito che spetta all'accusa provare l'elemento soggettivo anche nel caso in cui la fattispecie criminosa venga posta in essere da , negando la presenza di un'inversione dell'onere della prova, considerato da autorevole dottrina una violazione del principio di non colpevolezza e attestando un mero onere di allegazione in capo alla difesa.

[108] I modelli organizzativi rappresentano il "supporto materiale" della colpa di organizzazione, in questi termini PALIERO, PIERGALLINI, *La colpa di organizzazione*, in *Resp. Amm. Soc. ed enti*, 2006, 170.

[109] In questi termini PALIERO, *La società punita: del come, del perché e del per cosa*, in Riv. It. dir., e proc. pen., 2008, 1542; PULITANÒ, *La responsabilità da reato degli enti: i criteri di imputazione*, in *Riv. It. dir. Proc. pen*., 2002, 415.

[110] Cfr. DI GIOVINE, *Il criterio di imputazione soggettiva*, in LATTANZI, SEVERINO (a cura di), *Responsabilità da reato degli enti*, cit., 205.

La scelta sul *si et quomodo* predisporre un MOG è rimessa in gran parte all'autonomia decisionale degli enti privati. Lo dimostra, in primo luogo, la circostanza per cui l'adozione di un modello organizzativo si configura, nella maggior parte dei casi, come un onere e non un obbligo[111]: l'obiettivo del decreto consiste, infatti, nell'incentivare l'ente ad organizzarsi per prevenire la commissione di reati nel tessuto aziendale in cambio di benefici sanzionatori ma se lo stesso dovesse rinunciare ad investire in termini di *compliance*, non sussisterebbe alcuna sanzione quale diretta conseguenza della decisione. Le eccezioni alla regola sono poche: i modelli organizzativi vengono considerati un requisito necessario da alcune legislazioni regionali al fine di ottenere o mantenere l'accreditamento in settori specifici[112], sono specificamente richiesti per l'accesso alla quotazione nel Segmento Titoli con Alti Requisiti (STAR) ed in ultimo rappresentano un elemento di valutazione ai fini del *rating* di impresa[113] secondo quanto previsto dal Codice degli appalti.

In secondo luogo, ampi margini di libertà vengono lasciati all'organizzazione a struttura complessa nella predisposizione del MOCG. Il decreto 231, infatti, si limita a fornire «l'ossatura» del modello[114], inidonea da sola a guidare pedissequamente i destinatari del decreto nella predisposizione del modello organizzativo in quanto si sostanzia in un numero esiguo di prescrizioni formulate in maniera generica[115].

È' il comma 2 dell'art. 6 del d.lgs. 231/2001 ad incardinare gli elementi che devono fungere da scheletro di ogni modello organizzativo.

---

[111] V. GULLO, *I modelli organizzativi*, in LATTANZI, SEVERINO (a cura di), cit., 242.
[112] Si fa riferimento, in particolare, al settore sanitario
[113] Per *rating* di impresa si fa riferimento alla valutazione della capacità delle imprese di poter accedere alle gare pubbliche effettuata dall'ANAC
[114] Cfr. FIDELBO, *L'accertamento dell'idoneità del modello organizzativo in sede giudiziale*, in A.M STILE, MONGILLO, G. STILE (a cura di), *La responsabilità da reato degli enti collettivi: a dieci anni dal d.lgs. n. 231/2001*, Napoli, 2013, 173 ss; BIRRITTERI, *Big Data Analytics e compliance anticorruzione*, cit., 298
[115] Cfr. MANACORDA, *L'idoneità preventiva dei modelli di organizzazione*, cit., 66.

La prima prescrizione consiste nell'individuazione delle attività che possono essere considerate a rischio[116] di commissione dei uno dei reati tassativamente contemplati dagli articoli 24 e seguenti del decreto.

L'ente deve pertanto procedere alla c.d. mappatura del rischio[117] che consta di tre momenti differenti. Si richiede *in primis* un'analisi interna volta ad individuare le aree maggiormente esposte al rischio-reato, le quali si declinano diversamente a seconda dell'attività svolta dall'impresa, dell'articolazione interna allo stesso, dalla sua collocazione geografica e delle vicende passate idonee ad influenzare i processi futuri[118].

In secondo luogo, l'ente deve passare in rassegna le disposizioni normative concernenti i reati presupposto e delineare le possibili modalità di violazione delle stesse alla luce dell'attività economica esercitata.

In ultimo, l'organizzazione a struttura complessa gode di un'ampia discrezionalità nello stabilire un tasso di rischio accettabile, partendo dal presupposto che l'azzeramento dello costituisce un obiettivo inverosimile[119].

Il secondo *step* da seguire nella creazione di un MOG consiste nella c.d. procedimentalizzazione, vale a dire nella previsione di specifiche regole e protocolli diretti a programmare la formazione prima e l'attuazione poi delle scelte operate dall'ente, con l'obiettivo di trasformare l'intero percorso decisionale in un vero e proprio «processo»[120]. Questa prescrizione si

---

[116] Per "rischio" si intende qualsiasi variabile o fattore che nell'ambito dell'azienda, da soli o in correlazione con altre variabili, possano incidere negativamente sul raggiungimento degli obiettivi indicati dal decreto 231, in questi termini le Linee Guida redatte da Confindustria e aggiornate al 2021, 39.

[117] Sul punto v. GULLO, *I modelli organizzativi*, in LATTANZI, SEVERINO (a cura di), *Responsabilità da reato*, cit., 254.

[118] In argomento sempre GULLO, *I modelli organizzativi*, in LATTANZI, SEVERINO, *Responsabilità da reato*, cit., 255.

[119] Il legislatore non si è mai pronunciato in materia e a sopperire a tale lacuna normativa sono intervenute le linee guida di Confindustria. Alla luce delle stesse, la soglia concettuale di accettabilità, nei casi di reati dolosi, è rappresentata da un sistema di prevenzione tale da non poter essere aggirato se non fraudolentemente. Questa soluzione è in linea con la logica della "elusione fraudolenta" del modello organizzativo quale esimente espressa dal decreto 231 ai fini dell'esclusione della responsabilità amministrativa dell'ente (art. 6, comma 1, lett. c, "le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione"), v. Linee Guida Confindustria aggiornate al 2021, 40.

[120] V. PIERGALLINI, *i modelli organizz*ativi, in AA. VV., LATTANZI (a cura di), *Reati e responsabilità*, cit., 156.

sostanzia in una serie di prassi quali il coinvolgimento di diverse figure professionali che fungano da centri intermedi di imputazione della responsabilità[121], l'analitica divisione dei poteri, la segregazione delle funzioni ed infine la regolamentazione analitica dei processi, il tutto con l'obiettivo di escludere che una singola persona fisica detenga un potere decisionale illimitato e di rendere facilmente ricostruibile l'interno processo che ha condotto ad una decisione finale[122].

La terza indicazione contemplata dall'art 6 comma 2 del d.lgs. 231/2001 ha ad oggetto i flussi finanziari: il legislatore prescrive alla persona giuridica di individuare modalità di gestione degli stessi volte ad impedire la commissione dei reati. In quest'ottica risulta utile stabilire a monte i poteri di spesa in capo ai singoli, prevedere un meccanismo preventivo di autorizzazioni nonché predisporre modalità volte alla tracciabilità delle risorse finanziarie così da controllarne il corretto impiego[123].

Un ultimo elemento imprescindibile per un modello che intenda ottenere un giudizio positivo circa la sua idoneità attiene ai flussi informativi e si sostanzia nella previsione di specifici obblighi di informazione nei confronti dell'Organismo di vigilanza deputato a vigilare sul funzionamento e l'osservanza dei modelli[124]. All'indubbia centralità attribuita dal legislatore del 2001 all'OdV, non corrisponde altrettanta completezza regolamentare. Il decreto legislativo tace del tutto circa la sua composizione, il suo funzionamento e le modalità di conduzione dei controlli e alle suddette lacune sopperiscono le Linee Guida delle associazioni di categorie, la Parte Generale del modello e le indicazioni estrapolate da alcune pronunce giurisprudenziali[125].

---

[121] In modo da non concentrare la facoltà di decidere nelle mani di una singola persona fisica.

[122] Sul punto v. GULLO, *I modelli organizzativi*, in LATTANZI, SEVERINO (a cura di), *Responsabilità da reato*, cit., 257.

[123] V. GULLO, *I modelli organizzativi*, in LATTANZI, SEVERINO (a cura di), *Responsabilità da reato*, cit., 257.

[124] Ex art 6 co. 2 lett. D d.lgs 231/2001

[125] Per fare un esempio di come le pronunce giudiziali abbiano dovuto sopperire al silenzio normativo: Il Trib. Riesame Parma in data 26 maggio 2015 ha ritenuto il modello adottato dalla società imputata inidoneo in ragione della previsione di un OdV in composizione monocratica, da

Le uniche indicazioni normative sul punto[126] sono contemplate dall'art. 6 del decreto 231, articolo dedicato al criterio di imputazione soggettiva della responsabilità dell'ente nel caso in cui siano i soggetti apicali ad aver integrato la fattispecie criminosa. Alla luce dello stesso, si attribuiscono all'OdV specifici poteri di iniziativa e controllo, lo si incarica di vigilare sul funzionamento, sull'osservanza e sull'aggiornamento del MOG[127] e lo si onera di farsi carico delle istanze informative provenienti dai soggetti che operano a vario titolo nell'ente, come specificato nella lettera d.

In ultimo, i commi 4 e 4bis del medesimo articolo garantiscono la possibilità alle piccole e medie imprese di demandare i compiti spettanti all'OdV all'organo dirigente mentre le suddette funzioni possono essere attribuite nelle società di capitali al collegio sindacale, al consiglio di sorveglianza o al comitato per il controllo della gestione, a seconda che abbiano adottato rispettivamente il modello tradizionale, monistico o dualistico.

Per concludere, con l'obiettivo di rendere effettive le indicazioni prospettate nelle lettere precedenti, l'art. 6 suggerisce all'ente di introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello[128] ed infine, a partire dal 2017 si rende necessario prevedere specifici canali di segnalazione di condotte illecite, il c.d. *whistleblowing*[129], nonché meccanismi volti a tutelare il *whistleblower*, vale a dire il soggetto segnalante[130].

Una pratica che è stata resa ancor più centrale con l'entrata in vigore del d.lgs. 24/2023, provvedimento normativo che oltre ad estendere l'elenco

tale pronuncia si desume che un MOG, per essere considerato idoneo, deve affidare le funzioni di controllo e aggiornamento ad un Organismo di Vigilanza in composizione collegiale.

[126] Il decreto contiene infatti una disciplina scarna in relazione all'Organismo di vigilanza, per di più foriera di molteplici dubbi interpretativi, così PIERGALLINI, *I modelli organizzativi*, cit. 168.

[127] Ai sensi dell' art 6 co. 1 lett. b d.lgs 231/2001

[128] Ex art 6 co 2. Lett. E D.lgs 231/2001

[129] il cui naturale destinatario è l'ODV seppur manchi una specifica indicazione in tal senso da parte del decreto

[130] Per un approfondimento sul punto si rimanda all'ultimo paragrafo del presente capitolo in materia di *internal investigations*.

delle condotte meritevoli di segnalazione[131], rafforza l'insieme delle tutele in favore dei segnalanti, ampliando dapprima il novero degli stessi, affidando la gestione della segnalazione ad un ufficio aziendale autonomo e costituito da personale specificatamente formato o, in alternativa ad un soggetto esterno qualificato e prevedendo adempimenti rilevanti in materia di protezione dei dati personali[132].

Ulteriori indicazioni contenute nel d.lgs. 231/2001 volte ad orientare l'ente nelle attività di predisposizione ed efficace attuazione del modello organizzativo sono contenute nell'art 7 comma 3. Il legislatore richiede all'ente di prevedere misure idonee a garantire lo svolgimento delle attività nel rispetto della legge, tenendo conto della natura della persona giuridica, della dimensione dell'organizzazione nonché del tipo di attività esercitata dall'impresa.

È nel comma 4 del medesimo articolo che il legislatore fornisce due prescrizioni principali a garanzia dell'efficace attuazione dei presidi organizzativi incardinati nel modello. Si richiede, in primo luogo, che l'ente predisponga verifiche periodiche del MOG, con conseguenti modiche strutturali nel caso in cui si riscontri una violazione delle regole o si verifichi un fisiologico cambiamento in termini organizzativi o a livello di attività posta in essere. In secondo luogo, viene caldeggiata la predisposizione di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure sopra indicate.

Per concludere, merita di essere menzionato quanto stabilito dal comma 3 dell'art 6, vale a dire la possibilità di predisporre il modello organizzativo alla luce dei codici di comportamento adottati dalle associazioni di categoria. Questa scelta va comunicata al Ministero della Giustizia che, di concerto con gli altri Ministeri competenti, può formulare osservazioni sull'idoneità preventiva dei modello presentato entro 30 giorni.

---

[131] Il d.lgs. 24/2023 introduce anche le violazioni lesive degli interessi dell'Unione europea, dell'interesse pubblico o della Pubblica Amministrazione

[132] V. BORTOLOTTO, *In G.U. il d.lgs. 24/2023 attuativo della Direttiva Whistleblowing*, in *Altalex*, 2023; Rapporto PWC sul Whistleblowing alla luce delle novità introdotte dal d.lgs. 24/2023 in attuazione della Direttiva UE 2019/1937, *https://www.pwc.com*

Le linee guida formulate dalle associazioni di categoria, in particolar modo da Confindustria e ABI, hanno rivestito e tuttora rivestono un ruolo di fondamentale importanza. Le stesse sopperiscono alle lacune normative in materia, fornendo indicazioni idonee ad orientare le imprese nella predisposizione dei modelli organizzativi che nel tempo sono diventate *best practices* da replicare[133].

Quanto alla struttura, ogni modello organizzativo dovrebbe contemplare due diverse componenti: una Parte Generale e una Parte Speciale.

La prima è stata definita la «carta d'identità»[134] dell'ente proprio perché una volta pubblicata è utile a rendere lo stesso facilmente identificabile all'esterno. La Parte generale contiene, pertanto, informazioni in merito all'articolazione dell'ente, indica l'area di *business* in cui opera lo stesso, mostra la dislocazione geografica delle sue sedi, specifica la sussistenza di un'eventuale quotazione in borsa, illustra la forma giuridica adottata dalla persona giuridica e fornisce informazioni in merito al sistema di deleghe e poteri adottato dall'impresa, quale fulcro dell'attività di procedimentalizzazione sopra illustrata.

Le Linee Guida redatte da Confindustria hanno contribuito a strutturare la Parte generale del MOG in tre distinte sezioni: Il Codice Etico, il Sistema di controllo interno e il Sistema Normativo[135].

Quanto al Codice etico, quest'ultimo consente di illustrare il compendio di valori al quale si ispira l'ente nell'esercizio dell'attività di impresa. Si tratta di un documento ufficiale, generalmente predisposto dal massimo vertice dell'ente, il quale si sostanzia in una serie di adempimenti informativi.

In primo luogo, il Codice etico contiene la *mission* dell'impresa, le modalità per conseguirla e l'insieme dei diritti, dei doveri e delle

[133] Cfr. GULLO, *I modelli organizzativi*, in LATTANZI, SEVERINO (a cura di), cit., 264 ss;
[134] V. GULLO, *I modelli organizzativi*, in LATTANZI, SEVERINO (a cura di), cit., 266 ss.
In questi termini anche le Linee Guida redatte da Confindustria e aggiornate al 2021, *https://www.confindustria.it/home/policy/position-paper/dettaglio/linee-guida-modelli-organizzazione*
[135] Sul punto v. GULLO, *I modelli organizzativi*, in LATTANZI, SEVERINO (a cura di), cit., 265 ss.

responsabilità dell'ente nei confronti dei "portatori d'interesse"[136]. In secondo luogo, elenca sia i destinatari[137] che l'ambito di applicazione dello stesso. In aggiunta, illustra le norme di comportamento che consistono alternativamente in divieti e standard di comportamento. Il codice etico generalmente prosegue con la previsione delle indicazioni utili a garantire l'attuazione, il controllo e la diffusione dello stesso, fondamentali per mettere in pratica quanto teorizzato nei punti precedenti. In ultimo, il documento in esame contempla le diverse sanzioni esperibili nel caso in cui una delle previsioni contemplate venga violata. L'adozione di un Codice Etico completo di tutti gli elementi sopra indicati costituisce un sintomo dell'integrità aziendale, elemento considerato di fondamentale importanza da un numero sempre crescente di imprese[138], a prescindere dalla loro dimensione[139].

Passando all'analisi del Sistema di Controllo interno, quale secondo elemento che compone la Parte Generale del modello, va evidenziata sin da subito la presenza di una disciplina scarna in materia. Ne consegue che, anche in relazione a quest'ultimo elemento, sono venute in soccorso degli enti le linee guida predisposte dalle associazioni di categoria, in modo particolare da Confindustria[140].

---

[136] L'insieme dei soggetti che a vario titolo si interfacciano con l'organizzazione a struttura complessa come i dipendenti, i fornitori, i clienti, la Pubblica Amministrazione, gli eventuali azionisti e così via.

[137] Vale a dire l'insieme dei soggetti che devono conformare le proprie attività a quanto stabilito dal Codice Etico.

[138] Alla luce dell'intervista condotta nel 2017 a cura di EY, Il 97% delle imprese intervistate conferma l'importanza che la loro organizzazione agisca con integrità e che questo modus operandi venga riconosciuto anche dall'insieme dei consociati. Il fattore dell'*integrity* rappresenta un elemento di fondamentale importanza in primis poiché consente di prevenire la commissione degli illeciti ed il conseguente rischio di incorrere in sanzioni di vario tipo, in secondo luogo poiché rappresenta un vantaggio competitivo v. EY, *Integrity in the spotlight, the future of compliance, 15th Global Fraud Survey*, 2018, 18 ss. *https://www.ey.com/en_gl/assurance/how-to-drive-the-future-of-compliance-with-integrity-in-the-spotlight*

[139] In Italia è stato predisposto un PMI *Business Integrity kit* a cura del *business integrity forum* di *Trasparency international* Italia con l'obiettivo di diffondere i valori della trasparenza, integrità e anticorruzione nelle piccole e medie imprese, v. *https://businessintegrity.transparency.it/pmi_integrity_kit/*

[140] V. Linee guida Confindustria aggiornate al 2021 *https://www.confindustria.it/home/policy/position-paper/dettaglio/linee-guida-modelli-organizzazione*

Le *best practices* in materia precisano sin da subito che il sistema di controlli preventivi dovrà essere tale da garantire che i rischi di commissione dei reati siano ridotti ad un «livello accettabile»[141].

Vengono contemplati tre diversi livelli di controllo, dove l'ultimo degli stessi è pensato principalmente per le imprese a struttura complessa o di dimensioni medio-grandi. Il primo è svolto generalmente dal preposto o dirigente dell'ente ma, al qualora sussista la necessità di condurre verifiche specialistiche, può prevedere il coinvolgimento di risorse esterne alla persona giuridica e si sostanzia nell'insieme dei controlli c.d. di linea, orientati alla verifica delle misure di natura organizzativa e procedurale relative alla salute e sicurezza.

Il secondo livello di controllo è affidato da soggetti interni all'impresa competenti in materia, ai quali è richiesto di operare in rapporto di indipendenza rispetto all'organo che conduce i controlli di primo tipo. Questi ultimi si sostanziano nell'attività di monitoraggio sul processo di gestione e controllo dei rischi legati all'operatività del sistema.

Il terzo livello di controllo viene effettuato dall*'Internal Audit*, organismo che si occupa di operare valutazioni indipendenti in merito alla struttura e al funzionamento complessivo dell'intero Sistema di Controllo Interno adottato dall'ente e di prospettare eventuali miglioramenti dello stesso in appositi piani predisposti in concerto con il *Management*[142].

L'ultimo elemento contenuto della Parte Generale del modello organizzativo è rappresentato dal Sistema Normativo, vale a dire un microcosmo di regole interne all'ente che consta di statuti, circolari, procedure ed istruzioni da implementare [143]

La Parte Speciale rappresenta la seconda componente di un modello organizzativo. Quest'ultima contempla i cosiddetti protocolli preventivi

---

[141] Le Linee Guida redatte da Confindustria e aggiornate al 2021, 50. *https://www.confindustria.it/home/policy/position-paper/dettaglio/linee-guida-modelli-organizzazione*

[142] Cfr. Linee Guida redatte da Confindustria e aggiornate al 2021, *https://www.confindustria.it/home/policy/position-paper/dettaglio/linee-guida-modelli-organizzazione*

[143] V. GULLO, *I modelli organizzativi*, in LATTANZI, SEVERINO (a cura di), cit., 266 ss.

specifici, anche conosciuti come *risk assesment* e *risk management*, volti a delineare le aree a maggior rischio-reato e a gestire lo stesso, riducendolo ad un livello di tollerabilità previamente stabilito.

La Parte Speciale può essere costruita per fattispecie di reato o per processi. Nella prima eventualità si parte dall'analisi delle fattispecie criminose tassativamente elencate nel decreto per poi prendere atto delle modalità idonee ad integrare gli stessi, individuare le principali aree a rischio, stabilire il tasso di probabilità di commissione degli illeciti e l'elaborazione dei profili di controllo. Nel secondo caso, al contrario, il punto di partenza è rappresentato da un processo specifico, dall'analisi del quale è possibile individuare i reati presupposto che hanno maggiori probabilità di essere commessi e gli altri elementi sopra illustrati[144].

2.1. *Risk analysis* per la mappatura delle aree a rischio commissione reati

Illustrate su un piano teorico le opportunità derivanti dall'utilizzo delle nuove tecnologie a supporto della *compliance* dell'ente, è bene interrogarsi sui possibili impieghi concreti delle stesse nelle diverse fasi di costruzione di un modello organizzativo precedentemente illustrate.

Gli algoritmi di intelligenza artificiale si configurano quale valido supporto già nella prima attività a cui l'ente deve adempiere, vale a dire la fase di mappatura dei rischi di commissione dei reati presupposto[145], da considerarsi quale primo requisito fondamentale di ogni modello organizzativo che ambisca ad un giudizio positivo circa la sua idoneità ai sensi dell'art 6 co. 2 lett. a) del d.lgs. 231/2001.

L'attività di identificazione dei rischi di commissione di reati quale primo momento nella generale operazione di mappatura, richiede l'analisi di una mole enorme di dati ed informazioni[146] in continua e rapida

[144] V. GULLO, *I modelli organizzativi*, in LATTANZI, SEVERINO (a cura di), cit., 266.
[145] Cfr. RUSSO, *I modelli di organizzazione, gestione e controllo*, cit., 90 ss; MORGANTE, FIORINELLI, *Promesse e rischi*, cit., 9 s; Della stessa opinione anche EY, *Global Forensic Data Analytics Survey 2018: How can you disrupt risk in an era of digital transformation*?, 2018; TREZZA, *L'Intelligenza Artificiale come ausilio alla standardizzazione*, cit., 3 s.
[146] Così BIRRITTERI, *Big Data Analytics e compliance anticorruzione*, cit., 290; SABIA, *Artificial intelligence and environmental criminal Compliance*, cit., 184;

evoluzione, tale da rendere le operazioni del *team* di esperti ad essa preposto particolarmente onerose, lente ed il più delle volte imprecise.

Una valida soluzione alle difficoltà[147] incontrate in questa fase di *risk assesment* è rappresentata dall'impiego dei nuovi *tools*, in modo particolare gli algoritmi di *big data analysis*[148]. Questi ultimi, in virtù della notevole capacità computazionale e di comparazione che li caratterizza, sono capaci di acquisire, analizzare e mettere in relazione enormi quantità di dati in maniera notevolmente più precisa e in tempi quantitativamente più ridotti rispetto alle tradizionali metodologie analogiche[149]. In aggiunta, le tecniche computazionali adoperate hanno raggiunto un tale grado di raffinatezza tecnologica da elidere ogni margine d'errore o possibilità di perdita di dati determinanti[150].

Gli algoritmi intelligenti applicati in tale frangente andrebbero a fungere da «microscopio»[151] della realtà d'impresa interna all'ente, garantendo la possibilità di portare a termine un'analisi dettagliata della stessa. Ne deriverebbe un «quadro iper-realista»[152] delle variabili determinati in questa fase nonché delle dinamiche societarie, utile ad intercettare ogni possibile fattore di rischio di commessione di uno o più reati idonei a configurare una responsabilità in capo all'ente. La *digital criminal compliance*, pertanto, darebbe la possibilità all'ente di interare al

[147] Sul punto v. BURCHARD, *Digital criminal compliance*, in ENGELHART, KUDLICH, VOGEL (a cura di), *Digitalisierung, Globalisierung und Risikoprävention*, 2021, Berlino, 745; in questa direzione anche QUEST, CHARRIE, CROO DE JONGH, ROY, *The risks and benefits of using AI to detect a crime*, in *Harvard Business review*, 2018, 5.

[148] La soluzione viene prospettata nel documento elaborato da EY, *Global Forensic Data Analytics Survey 2018: How can you disrupt risk in an era of digital transformation*? 2018, *https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/assurance/assurance-pdfs/ey-global-fda-survay.pdf* ; della stessa idea anche PWC, *Re-inventing internal controls in the digital age*, 2019, 10, in *www.pwc.com;* sul punto anche SABIA, *Artificial intelligence and environmental criminal Compliance*, cit., 181 ss.

[149] In argomento v. PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in CADOPPI, CANESTRARI, MANNA, PAPA (*a cura di*), *Cybercrime*, 2019, Torino, 43 ss.

[150] V. BURCHARD, *Digital Criminal Compliance*, cit., 745

[151] Espressione utilizzata da BODEI, *Dominio e sottomissione. Schiavi, animali, macchine e intelligenza artificiale*, 2019, Bologna, 333.

[152] Cfr. FERRARESE, *Presentazione dell'edizione italiana di* GARAPON, LASSEGUE, *La giustizia digitale*, Bologna, 2021, 111 s, si fa riferimento alle potenzialità proprie dei nuovi paradigmi tecnologici di operare una «scansione» di un ente, una "radiografia" digitale dello stesso che consta di un insieme di dati da mettere in correlazione tra loro e da sfruttare per un'infinità di operazioni.

meglio il requisito dell'adeguatezza del modello[153], vale a dire la necessità che lo stesso venga predisposto in aderenza alle caratteristiche specifiche e alle peculiarità di quest'ultimo[154].

L'attività di identificazione dei rischi può trarre un concreto beneficio altresì dall'impiego di tecniche di *predictive analysis*. Queste ultime, infatti, non si limitano a fotografare la realtà circostante ma, attraverso l'analisi delle cause che hanno determinato le condotte illecite del passato, consentono di effettuare previsioni sui probabili rischi futuri di commissione dei reati[155], andando così a potenziare notevolmente l'efficacia di questi primo adempimento organizzativo.

Procedendo nell'analisi dei possibili impieghi delle nuove tecnologie nella fase di mappatura dei rischi, è possibile affermare che gli algoritmi di IA possano configurarsi quali validi alleati del personale specializzato anche in relazione al secondo *step* della stessa, ovvero quello dell'analisi delle norme riguardanti i reati contemplati dagli artt. 24 ss. del d.lgs. 231/2001 nonché dell'esame delle possibili modalità idonee ad integrare gli stessi[156].

In relazione al primo profilo[157], le tecnologie di AI potrebbero essere impiegate nell'attività di *Regulatory detection* al fine di delineare un quadro competo delle normative in vigore e di avere contezza dei ricorrenti aggiornamenti in merito[158]. I nuovi *tools* andrebbero, inoltre, a facilitare le operazioni di raccolta della documentazione grazie ai sistemi di Ricerca semantica *smart*, i quali, a partire da una parola o da un concetto, consentono di rilevare tutti i file che risultano essere inerenti agli stessi. In aggiunta, gli algoritmi di intelligenza artificiale potrebbero essere adoperati nell'attività di *Impact Analyis* da declinarsi in un triplice ordine: una classificazione

[153] Il requisito dell'adeguatezza è da annoverare tra gli elementi che fondano il giudizio di idoneità dell'ente, per un'analisi sul punto si rimanda all'ultimo paragrafo del presente capitolo
[154] Cfr. MORGANTE, FIORINELLI, *Promesse e rischi*, cit., 10, dove si fa riferimento all'utilità dei nuovi paradigmi tecnologici per la "customizzazione" del modello organizzativo
[155] Sul punto v. PWC, *Il Modello 231/01 tra innovazioni normative e tecnologiche*, cit., 8; SABIA, *Artificial intelligence and environmental criminal compliance,* cit., 184
[156] In argomento v. GULLO, *I Modelli organizzativi,* cit. 255.
[157] Si fa riferimento all'attività di dell'analisi delle norme riguardanti i reati contemplati dagli artt. 24 ss. del d.lgs 231/2001
[158] Cfr. PWC, *Il Modello 231/01 tra innovazioni normative e tecnologiche,* cit., 8;

delle *policy* interne e un loro confronto con la normativa esterna, una comparazione tra versioni normative diverse, una classificazione dei requisiti regolamentari in relazione alla struttura organizzativa o del processo specifico. Infine, adoperare i *software* in questa fase, alla luce delle analisi condotte sui *cluster* di dati, consentirebbe di intercettare gli "*hot topic*", vale a dire i possibili ambiti che saranno oggetto di regolamentazione futura[159], dando la possibilità alle persone fisiche preposte alla predisposizione del MOG di prevedere gli interventi del legislatore.

Quanto al secondo profilo[160], risulta utile adoperare tecniche di *data mining* le quali, operando correlazioni tra una pluralità di fonti, consentono di rintracciare i *trend* relativi alle modalità impiegate nella commissione degli illeciti nel passato nonché, di nuovo, algoritmi di *predictive analysis* utili ad effettuare previsioni circa le probabili condotte a carattere criminoso, alla luce della casistica precedentemente passata in rassegna[161].

Gli algoritmi di intelligenza artificiale potrebbero validamente supportare anche la terza attività ricompresa nella fase di mappatura del rischio, vale a dire quella orientata a stabilire una soglia di rischio-reato. Si è già detto sul punto che non esiste una disposizione legislativa che fissi un parametro ben preciso[162] e che l'unica indicazione in materia viene fornita dalle Linee Guida di Confindustria, le quali, in relazione ai reati dolosi, fanno coincidere lo stesso con il requisito dell'elusione fraudolenta[163]. Al fine di ridurre l'incertezza giuridica relativa al parametro in questione, i nuovi paradigmi tecnologici, in particolar modo quelli che si avvalgono delle tecniche di *Big Data Analysis*, potrebbero delineare una panoramica delle soluzioni adottate dalle imprese più virtuose nonché dalle disposizioni

[159] Soluzione prospettata da PWC nel documento dal titolo *Smart Compliance, un approccio evoluto per la gestione del rischio di non conformità* pubblicato nel 2022 in *https://pwc.com*
[160] Si fa riferimento all'attività di analisi delle possibili modalità idonee ad integrare i reati enumerati nel decreto 231
[161] V. PWC, *Il Modello 231/01 tra innovazioni normative e tecnologiche*, cit., 8;
[162] Autorevole dottrina non condivide il silenzio del legislatore sul punto, v. GULLO, *I modelli organizzativi*, cit., 255
[163] «Il modello deve risultare idoneo a resistere sino alla sua elusione fraudolenta», v. Linee Guida Confindustria aggiornate al 2021; GULLO, *I modelli organizzativi*, in LATTANZI, SEVERINO (a cura di), cit., 255.

legislative in vigore negli altri Paesi e fornire dei suggerimenti al legislatore sul punto.

All'utilizzo di algoritmi di intelligenza artificiale, in modo particolare quelli di *Big Data Analysis*, sembrano già ricorrere diverse persone giuridiche sia pubbliche che private. Queste ultime hanno la propria sede principale prevalentemente nei paesi anglosassoni e si avvalgono dei nuovi paradigmi tecnologici per la prevenzione dei reati corruttivi[164].

In relazione alle altre tipologie di fattispecie criminose, solo di recente si è prospettata l'opportunità di avvalersi dei *tools* intelligenti per la loro efficace prevenzione. I reati i cui appare opportuno far riferimento alla *digital criminal compliance* sono, in modo particolare, i reati ambientali, fattispecie criminose che costituiscono reati presupposto in quanto contemplati dall'art. 25-*undecies* del decreto legislativo 231/2001.

La dottrina ha osservato quanto gli strumenti di AI potrebbero essere d'aiuto alle *corporations* per prevenire e minimizzare gli impatti ambientali delle attività industriali i quali, al superamento delle soglie previste dalla legge, sono idonei a determinare una responsabilità penale per l'impresa. I *software* basati sull'intelligenza artificiale potrebbero monitorare in maniera costante la qualità dell'aria, dell'acqua e dell'ambiente e andrebbero a rendere l'attività *risk assesment* più accurata e tempestiva, così consentire all'ente di prevenire il rischio-reato e non incorrere in alcuna forma di responsabilità[165].

Al giorno d'oggi sono stati elaborati diversi *software* con l'obiettivo di mappare il rischio reato, uno di questi è rappresentato da Valore 24, una *web application* elaborata con l'obiettivo di supportare l'ente nelle operazioni di predisposizione di un modello organizzativo, in modo particolare nell'attività di *risk assesment*[166].

---

[164] Per un approfondimento sul punto v. BIRRITTERI, *Big Data Analytics e compliance anticorruzione*, cit., 289 ss.

[165] In argomento v. SABIA, *Artificial intelligence and environmental criminal compliance,* cit., 179 ss.

[166] Quanto alle funzionalità dello stesso v. *https://valore24.ilsole24ore.com/avvocati/231/*

2.2 Strumenti di Monitoraggio Automatico (SMA) per la procedimentalizzazione delle attività e delle decisioni interne

L'impiego dei nuovi paradigmi tecnologici si dimostra vantaggioso anche in relazione al secondo elemento costitutivo di un modello organizzativo alla luce di quanto stabilito dall'art 6 co. 2 lett b) sia sotto il profilo organizzativo che sotto il profilo del controllo[167].

Il primo valido utilizzo degli algoritmi di intelligenza artificiale riguarda la fase di procedimentalizzazione vera e propria, vale a dire la predisposizione delle regole e dei protocolli volti a programmare la attività in azienda e a regolare i processi decisionali che interessano l'ente[168].

I *tools* intelligenti, infatti, consentirebbero di minimizzare il rischio di violazione delle normative in vigore poiché in grado di ricomprendere divieti, soglie ed obiettivi, così da strutturare le operazioni da compiere ed organizzare le decisioni da assumere in *compliance* con le leggi, i regolamenti e le *best practices* elaborate dalle associazioni di categoria[169].

Il secondo importante beneficio connesso alla digitalizzazione delle attività nell'impresa consiste nella possibilità di monitorare costantemente i processi di formazione e attuazione delle decisioni che interessano l'ente[170] così da rilevare prontamente anomalie, incongruenze, violazioni delle norme in vigore e integrazione di fattispecie criminose[171].

Il controllo pervasivo sulle diverse attività poste in essere nel contesto aziendale è reso possibile, in modo particolare, dall'utilizzo di sistemi di monitoraggio automatico (SMA)[172], vale a dire strumenti che basano su tecniche e *software* innovativi, quali l'*intelligence* su fonti aperte, algoritmi di intelligenza artificiale, e i sistemi a registro distribuito, i quali

---

[167] Sul punto v. TREZZA, *L'Intelligenza Artificiale come ausilio alla standardizzazione,* cit., 3.
[168] Cfr. SABIA, *Artificial intelligence and environmental criminal compliance,* cit., 180.
[169] Secondo quanto prospettato da PWC, *Re-inventing internal controls in the digital age*, 2019, 10, in *www.pwc.com*
[170] V. SABIA, *Artificial intelligence and environmental criminal Compliance,* cit., 179 s. con specifico riferimento alle decisioni assunte dagli enti con l'obiettivo di prevenire i reati ambientali.
[171] Cfr. RUSSO, *I modelli di organizzazione, gestione e controllo. Letteratura, prassi e innovazioni tecnologiche*, cit., 95
[172] sul punto v. D'AGOSTINO, *Criminal Compliance e nuove tecnologie*, in corso di pubblicazione, 12.

andrebbero messi a disposizione dell'Organismo di vigilanza[173] al fine di facilitare e potenziare l'attività generale di controllo attraverso l'analisi dei dati a disposizione.

Un primo strumento riconducibile alla famiglia dei sistemi di monitoraggio automatico è rappresentato da una tipologia di *software* capace di elaborare *alert* indirizzati all'Organismo di vigilanza, da considerarsi, alla luce dei seppur scarni riferimenti normativi, naturale destinatario degli stessi. Gli *alert* automatici consistono in segnalazioni utili ad evidenziare anomalie nei comportamenti[174], discostamenti dalla procedura ordinaria fissata, ritardi rispetto alle tempistiche previste e così via, tutti elementi prodromici alla commissione di un reato o elementi costituivi dello stesso, a seconda del caso specifico. Avvalendosi delle tecnologie in esame, l'ente avrebbe la possibilità di intervenire tempestivamente e scongiurare la verificazione di una fattispecie criminosa nel tessuto aziendale o, se già verificatosi in concreto, ricostruire più agevolmente i profili di responsabilità in capo alle persone fisiche coinvolte.

Per fornire un esempio concreto in merito al funzionamento dello stesso è utile riportare il seguente *case study*. L'ente che nel caso di specie intende prevenire la commissione di reati presupposto nell'esercizio delle sue attività è un istituto bancario. La prima fase di mappatura dei rischi-reato evidenzia quale principale fattispecie criminosa di probabile integrazione il reato di ostacolo all'esercizio delle funzioni delle Autorità pubbliche di vigilanza[175], integrabile in caso di inottemperanza al dovere di comunicare mensilmente determinati dati relativi ad operazioni poste in essere dalla Banca. Al fine di prevenire lo stesso, si prospetta utile il ricorso ad un sistema in grado di segnalare all'Organismo di vigilanza, *in primis*, eventuali discrepanze tra il comportamento concretamente tenuto dai

[173] Cfr. RUSSO, *I modelli di organizzazione, gestione e controllo. Letteratura, prassi e innovazioni tecno logiche*, cit., 95

[174] I *software* in grado di analizzare i comportamenti umani prendono il nome di *Behaviour analysis.*

[175] Il reato di ostacolo all'esercizio delle funzioni dell'autorità di vigilanza costituisce uno dei reati presupposto idonei a configurare una responsabilità in capo all'ente in quanto è contemplato nell'art contemplato dall'art. 25-ter d.lgs 231/2001

soggetti che operano in banca con quello "doveroso" alla luce delle procedure ordinarie predisposte; in secondo luogo, l'insieme degli atteggiamenti sintomatici dell'intenzione di omettere determinate comunicazioni ed infine i casi di violazione delle tempistiche stabilite dal modello organizzativo adottato[176].

Un ulteriore strumento idoneo a potenziare il controllo dell'OdV sulle diverse procedure stabilite dal MOG è rappresentato dalle tecnologie a registro distribuito (DLT)[177]. Queste ultime si compongono di nodi utili a tenere traccia di tutti i passaggi che compongono ogni singola operazione registrata, dando la possibilità all'organismo di vigilanza di ricostruire agilmente le stesse, circostanza particolarmente utile nel caso in cui si debbano ridefinire i profili di responsabilità in capo alle persone fisiche che operano a vario titolo nell'ente[178].

Per concludere, autorevole dottrina ha prospettato un'ulteriore soluzione volta a semplificare la fase di procedimentalizzazione che si sostanzia nella predisposizione di «protocolli unitari» sempre a cura degli algoritmi di intelligenza artificiale. Si propone, dapprima, di riunire le imprese con il medesimo oggetto sociale e che operano nello stesso territorio per poi procedere ad un'unitaria mappatura delle aree a rischio volta ad individuare delle variabili comuni a tutte le società coinvolte. Le informazioni risultanti da questa fase potrebbero essere processate dai *tools* al fine di predisporre dei protocolli generalmente utilizzabili dalla cerchia degli enti coinvolti. Un'operazione di questo genere consentirebbe all'ente sia di velocizzare la suddetta seconda fase di predisposizione di un MOG idoneo che di risparmiare notevoli spese di *compliance*[179].

---

[176] Il seguente *case study* è stato prospettato da D'AGOSTINO, *Criminal Compliance e nuove tecnologie,* in corso di pubblicazione, 21.

[177] Per un'analisi approfondita sul punto si rimanda al primo capitolo del presente contributo

[178] Su punto v. D'AGOSTINO, *Criminal Compliance e nuove tecnologie*, in corso di pubblicazione, 17.

[179] In argomento v. TREZZA, *L'Intelligenza Artificiale come ausilio alla standardizzazione del modello 231,* cit., 4.

2.3 Algoritmi di *Natural Language Processing* (NLP), *Data Cassification* e *Data Loss Prevention* per il controllo dei flussi informativi

La gestione dei flussi informativi e la previsione di obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli rappresenta il terzo *step* nel processo di costruzione di un MOCG[180].

Digitalizzare la suddetta fase consentirebbe all'OdV di operare un controllo pervasivo sulle comunicazioni interne all'impresa nonché di essere prontamente informato sulla presenza di anomalie ed espressioni sintomatiche di un'intenzione a delinquere. È alla luce delle suddette potenzialità che risulta di agevole intuizione il principale beneficio connesso all'impiego di algoritmi di intelligenza artificiale nella gestione dei flussi informativi, vale a dire la possibilità per l'ente di non limitarsi a reagire a fronte della commissione di un reato da parte di un soggetto apicale o sottoposto ma di prendere provvedimenti in un momento precedente alla commissione dello stesso così da essere determinante nel prevenirne l'integrazione e scongiurare ogni forma di responsabilità prevista dal decreto 231[181].

Il principale *software* che si dimostra utile in questa fase è rappresentato dal *Natural Language Processing* (NLP). Quest'ultimo consta di algoritmi di IA capaci di analizzare e rappresentare il linguaggio naturale[182] nonché, con riferimento ai *tools* tecnicamente più sofisticati, di comprenderne il contenuto[183]. Alla luce degli ultimi approdi scientifici in materia, le tecnologie di NPL risultano pertanto in grado di portare a termine molteplici attività quali, tra le più rilevanti, la *text analysis*[184], la *text classification*[185], *l'intent monitoring*[186], la *smart search*[187] e la *sentiment*

[180] Alla luce di quanto stabilito dall'art 6 co.2 lett. (d) d.lgs. 231/2001.
[181] Sul punto v. D'AGOSTINO, *Criminal Compliance e nuove tecnologie*, in corso di pubblicazione, 2.
[182] Sul punto v. JAIN, KULKARNI, SHAH, *Natural Language Processing*, in *International Journal of Computer Sciences and Engineering*, 2018, 1. *www.ijcseonline.org*
[183] Si parla in questo caso di *Natural language understanding*
[184] Vale a dire l'analisi di un testo e la capacità di rilevare un elemento specifico
[185] Implica l'interpretazione di un testo così da classificarlo in una determinata categorie
[186] Fa riferimento alla comprensione di un testo per prevenire i comportamenti futuri
[187] Implica la ricerca intelligente in archivi

analysis[188], operazioni che si dimostrano particolarmente per le imprese, le quali dimostrano un sempre maggiore interesse nell'adottarle nel contesto aziendale[189].

I *tools* supportati da tecnologie di *Natural Language Processing* che si dimostrano più idonei a supportare la *compliance* dell'ente per come delineata dal d.lgs 231/2001 sono quelli di *Data Classification* e *Data Loss Prevention*. La prima declinazione di NLP si avvale di algoritmi di IA per effettuare ricerche dettagliate su prospetti testuali al fine di rintracciare i c.d. dati sensibili nel *database* e con l'obiettivo di classificare gli stessi a seconda del livello di rischio che presentano.[190] La suddetta classificazione rappresenta un valido supporto agli addetti ai lavori nella scelta della tipologia di controlli da effettuare sulle operazioni che coinvolgono i dati in questione, i quali saranno di intensità diversa a seconda dell'importanza di questi ultimi[191]. Un'accurata ponderazione delle attività di controllo alla luce delle evidenze concrete consentirebbe all'ente di gestire al meglio il personale nonché le risorse destinare a questa specifica fase di *compliance.*

Quanto alla tecnologia di *Data Loss Prevention*, quest'ultima garantisce una completa protezione dell'intero patrimonio informativo aziendale, minimizzando il rischio di manomissione dei dati sensibili nonché di perdita e di condivisione non autorizzata degli stessi[192]. Avere la garanzia dell'integrità dei *database* contenenti l'intero compendio di informazioni utili rappresenta un evidente vantaggio per l'ente, in modo particolare qualora voglia intraprendere un'attività di *internal investigation* o nel caso in cui sia onerato di produrre evidenze probatorie in giudizio.

---

[188] Vale a dire il rilevamento dell'umore a partire da un dato testuale

[189] Sul punto v. REDAZIONE OSSERVATORI DIGITAL INNOVATION, *Natural Language Processing (NPL): come funzione l'elaborazione del linguaggio naturale*, in osservatori.net Politecnico di Milano, 2021. *https://blogosservatori.net*

[190] In argomento v. D'AGOSTINO, *Criminal Compliance e nuove tecnologie*, in corso di pubblicazione, 28.

[191] Sul punto v. PWC, *Re-inventing internal controls*, cit., 2 ss.

[192] Alla luce del rapporto CLUSIT 2020, i sistemi di *Data Loss Prevention* si collocano sul podio delle tecnologie utilizzate dalle imprese italiane per proteggere il patrimonio informativo dell'impresa, in modo particolare dai cyberattacchi v. Rapporto Clusit 2020 sulla sicurezza ICT in Italia, 61.

Tra gli utilizzi più efficaci dei suddetti presidi tecnologici, è possibile menzionare l'analisi delle e-*mail* aziendali funzionale alla loro classificazione, l'acquisizione di informazioni da documenti nella disponibilità dell'ente, la rilevazione di parole sintomatiche di un'intenzione a delinquere e addirittura la comprensione di un sentimento alla base di un dato testuale.

Le operazioni di controllo poste in essere dalle nuove teologie sulle comunicazioni che intercorrono tra i soggetti interni all'ente nonché tra questi ultimi e terze parti, risulterebbero ancor più efficaci se coadiuvate da un meccanismo di *alert* capace di inviare una segnalazione all'OdV in presenza di parole sintomatiche di un'intenzione a delinquere o di contenuti sospetti.

Per fornire un esempio concreto di come operano le tecnologie sopra illustrate, è utile menzionare i seguenti *case study*.

Nel caso di specie, si richiede la gestione di un sistema informatico predisposto per lo svolgimento di procedure ad evidenza pubblica da parte di una Centrale di Committenza. I risultati dell'attività di mappatura del rischio dimostrano che tra i reati più soggetti di essere commessi in relazione alle operazioni in questo ambito vi siano quello di frode informatica a danno dello Stato o di altro ente pubblico[193] e quello di accesso abusivo a sistema informatico.[194] Una valida soluzione basata su paradigmi tecnologici utile a prevenire la prima fattispecie criminosa è rappresentata dai meccanismi di controllo e *matching* delle comunicazioni verificatesi nel contesto aziendale, metodologie utili a far emergere dinamiche di frode o corruttive.[195]

Per scongiurare il rischio di commissione della seconda fattispecie criminosa, si prospetta l'impiego di un *tool* capace di individuare le procedure e le offerte connesse a vario titolo al *business* della società e

[193] Il reato di frode informatica a danno dello Stato e di altro ente pubblico è disciplinato dall'art. 640-ter c.p, e costituisce un reato presupposto in quanto contemplato dall'art 24 d.lgs 231/2001

[194] Il reato di accesso abusivo a sistema informativo è disciplinato dall'art. 615-ter c.p. erappresenta un reato presupposto poiché preso in considerazione dall'art. 24-bis d.lgs 231/2001

[195] Sul punto v. D'AGOSTINO, *Criminal Compliance e nuove tecnologie*, in corso di pubblicazione, 19.

quindi esposte al rischio di accesso abusivo attraverso il sistema di *Data Classification* delle parole nel *database.* Il *software* in questione consente inoltre che solo la cerchia dei soggetti autorizzati abbia accesso ai documenti contenenti dati sensibili e dà la possibilità di rilevare e tenere traccia di tutte le copie e i download dei suddetti *file*[196].

Oltre ad un controllo su prospetti testuali quali *e-mail* e documenti, è possibile prospettare un monitoraggio delle conversazioni telefoniche attraverso la registrazione delle stesse, sempre previa informazione e autorizzazione da parte dei soggetti coinvolti. Tutte attività che comportano si indubbi benefici in termini di *compliance* della persona giuridica ma che celano, tuttavia, possibili rischi vi violazione del diritto alla *privacy* esplicitamente tutelato dal GDPR nonché l'articolo 4 dello Statuto dei Lavoratori[197].

2.4 *Distributed Ledger Tecnology* (DLT) per la tracciabilità' dei flussi finanziari

L'individuazione delle modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati rappresenta il quarto requisito contemplata dall'art 6 co. 2 lett. c) del d.lgs 231/2001.

Digitalizzare la gestione delle finanze interne all'ente comporta indubbi vantaggi[198] e lo strumento tecnologico che risulta più idoneo al conseguimento degli stessi è rappresentato dalle tecnologie a registro distribuito (DLT)[199]. Tali prospetti tecnologici, infatti, in virtù delle caratteristiche che li contraddistinguono[200], consentono di annotare dati sui registri distribuiti in maniera certa e sicura, garantiscono la data di registrazione degli stessi, non possono essere modificati senza il consenso dei soggetti firmatari, danno la possibilità di monitorare agevolmente le

[196] V. D'AGOSTINO, *Criminal Compliance e nuove tecnologie*, in corso di pubblicazione, 20.
[197] Per un approfondimento sul punto si rimanda al terzo capitolo del presente contributo che si occupa nello specifico di evidenziare le criticità proprie della *Digital criminal compliance*
[198] V. TREZZA, *L'Intelligenza Artificiale come ausilio alla standardizzazione,* cit., 3.
[199] Soluzione prospettata da PWC, Il Modello 231/01 tra innovazioni normative e tecnologiche, 2019 cit., 8.;
[200] In merito alla definizione e alle caratteristiche delle tecnologie DLT si rimanda al capitolo 1 del presente contributo

entrate e le uscite ed abilitano ad impedire una transazione se considerata illegittima, tutte potenzialità altamente funzionali per una corretta gestione delle risorse finanziarie.

Anche in relazione a questo adempimento contemplato dal decreto 231, risulta utile adottare un meccanismo di pronta segnalazione all'organo deputato al controllo e alla vigilanza in presenza di un valore che si discosta da quali previamente definiti, come, ad esempio, l'impegno di un ammontare di denaro superiore al potere di spesa concordato o irragionevolmente inferiore allo stesso.

Grazie ad una gestione digitalizzata delle risorse finanziarie, l'ente ha la possibilità di monitorare le operazioni di spesa condotte da apicali e sottoposti e di rilevare prontamente eventuali discostamenti ed anomalie dai parametri precedentemente definiti in sede di procedimentalizzazione delle attività nell'ottica di intervenire prontamente per evitare la commissione di reati nell'impresa.

2.5 *Due diligence* attraverso l'analisi su fonti aperte e le tecniche OSINT

Un ulteriore ambito capace di trarre un concreto beneficio dall'utilizzo dei nuovi paradigmi tecnologici è rappresentato dalla *due diligence*[201], vale a dire l'intero processo investigativo posto in essere da un ente al fine di raccogliere e verificare tutte le informazioni utili a valutare le attività aziendali[202]

I software che meglio saprebbero supportare i processi investigativi sopra indicati sono i c.d. sistemi OSINT[203]. La tecnologia in questione costituisce una branca dell'*intelligence* e si occupa di raccogliere e analizzare un vasto numero di dati presenti su "fonti aperte"[204].

[201] Espressione anglosassone che può essere tradotta con "dovuta diligenza"
[202] Sul punto v. SANTINI, *Due Diligence: Uno strumento imprescindibile nella valutazione delle aziende* in *Diritto.it*, 2019, 2.
[203] OSTINT è un acronimo che sta per *Open Source Intelligence*
[204] Vale a dire fonti accessibili a chiunque in quanto pubbliche e non classificate come ad esempio tutte le informazioni reperibili sul web, tramite i media tradizionali, che si trovano nei registri pubblici, negli atti giudiziari, nei documenti societari, etc.

Le tecnologie di *Open Source Intelligence* risultano potenziate grazie all'entrata in vigore della direttiva 2019/1024/UE recepita nel nostro ordinamento con il d.lgs. 200/2021. Tale intervento legislativo è orientato a stabilire norme comuni per la creazione di un mercato europeo dei dati di proprietà pubblica[205], incoraggiando la creazione di *Open Data*[206].
Nel provvedimento legislativo in esame, i dati aperti vengono suddivisi in quattro categorie principali: i dati dinamici, vale a dire documenti in formato digitale soggetti ad aggiornamenti frequenti o in tempo reale, i dati non dinamici; i dati della ricerca, utilizzati come prova nella ricerca scientifica ed infine la serie di dati di valore, il cui riutilizzo comporta notevoli benefici per la società[207].

La *Open Source Intelligence* consta di quattro distinte fasi. La prima è quella di *discovery*, nella stessa si verifica a raccolta di tutte le informazioni inerenti all'investigazione; la seconda prende il nome di *discrimination*, quest'ultima serve a scartare i dati superflui; la terza fase è quella della *distillation*, utile all'analisi dei dati ed in ultimo vi è la fase di *dissimination* nella quale avviene la redazione di un documento riassuntivo finale delle informazioni processate che risulteranno utili all'ente per decidere se intraprendere o meno una determinata operazione o per valutare quelle in atto[208].

A dimostrazione di come impiegare in concreto i suddetti *tools* in ambito *due diligence* è utile citare i seguenti *case study*. L'ente interessato ad avvalersi di algoritmi di intelligenza artificiale nella costruzione di un modello organizzativo idoneo è una Banca. A seguito dell'attività di mappatura dei rischi risulta che i reati che hanno più probabilità di essere

[205] Quanto delineato nel considerando 16 del della direttiva 2019/1024/UE, "promote the creation of data based on the principle of 'open by design and by default".
[206] Locuzione che non indica una tipologia ben precisa di dato ma che fa riferimento alla pratica di pubblicazione degli stessi al fine di renderli liberamente accessibili, riutilizzabili, leggibili con dispositivi elettronici e concessi in licenza, definizione contenuta in EUVocabularies;
[207] Così BONAVITA, CORTINA, *Direttiva Open Data: il problema dei formati e il "buco" sulla sicurezza*, in *Agenda digitale*, 2022 *https://www.agendadigitale.eu/sicurezza/direttiva-open-data-il-problema-dei-formati-e-il-buco-sulla-sicurezza/*
[208] Cfr. BONAVITA, CORTINA, *Direttiva Open Data: il problema dei formati e il "buco" sulla sicurezza*, in *Agenda digitale*, 2022 *https://www.agendadigitale.eu/sicurezza/direttiva-open-data-il-problema-dei-formati-e-il-buco-sulla-sicurezza/*

commessi sono quelli di corruzione attiva e di riciclaggio, disciplinati rispettivamente negli articoli 321 c.p. e 648-bis ss. e ricompresi nell'elenco tassativo dei reati presupposto idonei ad ascrivere una responsabilità in capo all'ente in quanto menzionati dagli articoli 25 e 25-octies del d.lgs 231/2001.

Per prevenire la commissione del reato di corruzione attiva, risulta utile predisporre un *software* basato sulle tecniche OSINT capace di rilevare le generalità dei soggetti pubblici che instaurano rapporti economici con l'istituto bancario. Il suddetto *tool* andrebbe affiancato sia da un paradigma tecnologico di *Data monitor*, capace di operare un controllo in tempo reale dei flussi informativi che intercorrono tra gli stessi, che da un meccanismo di *alert* volto ad avvisare tempestivamente l'OdV in presenza di irregolarità rilevate dal sistema[209].

Quanto ai reati di riciclaggio, finanziamento del terrorismo e delitti di criminalità organizzata, una valida soluzione digitale capace di prevenire gli stessi è rappresentata da una tipologia di *software* OSINT idoneo a ricavare da "fonti aperte" una serie di informazioni riguardanti i soggetti che intendono instaurare un rapporto economico con la banca. L'acquisizione delle notizie è funzionale a stabilire un punteggio di rischio per ciascuna persona fisica oggetto di analisi, il quale consentirà di decidere se entrare in affari o meno con la stessa. In caso di decisione affermativa, si dovrà procedere a controlli periodici funzionali a segnalare la sopravvenienza di nuove informazioni rilevanti, la cui frequenza e il cui grado di dettaglio dipendono dal *rating* di rischio del soggetto coinvolto.

A completare il quadro di misure orientate alla prevenzione dei reati, andrebbe adottato un meccanismo di report in *real time* all'organismo preposto, così da segnalare la sopravvenienza di anomalie, rischi e irregolarità.

Tra i *software* più diffusi in ambito *due diligence* ci sono il sistema CERICO e il *software* WORLD CHECK. Il primo è idoneo ad analizzare e valutare un *range* di dati allo scopo di effettuare una valutazione in merito

[209] Su punto v. D'AGOSTINO, *Criminal Compliance e nuove tecnologie*, in corso di pubblicazione, 20. V. BIRRITTERI, *Big Data Analytics e compliance anticorruzione*, cit., 295

ai rischi connessi ad una specifica operazione economica. I risultati dell'analisi vanno a confluire in un unico dato, il tasso di rischio, che servirà all'impresa per decidere se agire o meno[210]. Il secondo è un *tool* impiegato già da molteplici realtà per aiutare a identificare e gestire rischi di natura finanziaria, normativa e reputazionale[211].

2.6 Il *Regtech*

Come già anticipato nei paragrafi precedenti del presente contributo, i modelli tradizionali di *compliance* risultano sempre più inadeguati ad implementare il vasto e frammentario universo di normative in vigore.

È con l'obiettivo di comare le lacune proprie dei paradigmi analogici che è stata avvertita l'esigenza di sviluppare il *Regtech*[212], sostantivo che indica l'utilizzo del vasto panorama di nuove tecnologie per facilitare l'adempimento ai crescenti oneri normativi e di *compliance* in maniera più efficiente ed efficace rispetto alle tradizionali metodologie basate sul solo contributo umano[213].

Il fenomeno prende piede negli anni successivi alla crisi finanziaria del 2008, periodo in cui si assiste ad un proliferare di nuove disposizioni normative emanate con l'obiettivo di arginare le conseguenze derivanti dalla crisi economica del periodo. Il *Reghtech* nasce proprio con l'obiettivo di fornire un valido supporto ai soggetti destinatari[214] dell'ingente *corpus* regolamentare adottato nel settore finanziario[215] che ha previsto l'entrata in vigore di nuovi reati nonché l'adozione di provvedimenti *ad hoc* quali

[210] CERICO è un software fornito da Dow Jones Risk & Compliance, *www.dowjones.com*

[211] Per un approfondimento sulle modalità di funzionamento di WORLD CHECK v. *www.refinitiv.com*

[212] Termine che costituisce la crasi tra i sostantivi *regulation* e *tecnology*, vale a dire regolamentazione e tecnologia

[213] Sul punto v. FINANCIAL CONDUCT AUTHORITY, *Call for Input on Supporting the Development and Adopters of RegTech*, 2016; SABIA, *Artificial intelligence and environmental criminal Compliance*, cit., 181.

[214] Si trattava, nella gran parte dei casi, di società a struttura complessa di ingenti dimensioni sia in termini di estensione territoriale che di coinvolgimento di risorse umane, v. VIANELLI, VALENTI, *RegTech e Modelli 231: uno sguardo al futuro per un'esigenza presente*, in *Giurisprudenza Penale*, 2021, 4.

l'Anti-Money Laundering (AML), il *Know Your Customer (KYC)* ed il *Counter-terrorist Financing (CTF) policies*[216]

Nonostante le origini dello stesso e la circostanza per cui tutt'oggi il settore che contempla una maggiore adozione di soluzioni tecnologiche sia quello finanziario, il *RegTech* non deve essere concepito come un mero sottoinsieme[217] del *Fintech*[218], quest'ultimo implica infatti l'utilizzo di processi automatizzati non solo nell'ambito finanziario ma a tutti i settori improntati alla *compliance*.

Il *Reghtech* si avvale di molte tecnologie, diverse a seconda dell'ambito specifico in cui devono essere adoperate ma tutte riconducibili alla macrocategoria di intelligenza artificiale e tutte improntate a migliorare l'implementazione normativa ed i controlli operativi[219]. Avvalersi di soluzioni *Reghtech* implica molteplici benefici quali una sostanziale riduzione dei costi di implementazione, una maggiore efficienza nelle attività di compliance le quali, grazie ai nuovi paradigmi tecnologici utilizzati, si attuano in tempo reale ed infine un miglioramento nelle operazioni di controllo e monitoraggio[220].

Se il mercato europeo nell'ultimo quinquennio ha registrato una notevole crescita degli investimenti in materia *Regtech*[221], il mercato italiano risulta essere ancora essere molto ridotto in quanto questo settore ha preso piede nel nostro Paese solo di recente[222]. Sono 250 le aziende italiane che operano in ambito *Regtech*[223], due delle quali sono *ARisk* e *Ineo*.

La prima è un'azienda nata nel 2017 con il contributo del Politecnico di Torino. Quest'ultima si occupa di utilizzare gli algoritmi di AI, in modo

---

[216] Cfr. SABIA, *Artificial intelligence and environmental criminal Compliance*, cit., 182 s.
[217] V. SABIA, *Artificial intelligence and environmental criminal Compliance*, cit., 182.
[218] Se declinato al settore finanziario, è più indicato parlare di *Fintech "financial technology*", ossia lo sviluppo dei nuovi paradigmi tecnologici per rispondere alle esigenze della finanza, sul punto v. ARNER, BARBERIS, BUCKLEY, *FinTech, RegTech and the Reconceptualization of Financial Regulation, in Northwestern Journal of International Law & Business*, Hong Kong, 2016, 4 ss.
[219] Sul punto v. PWC, RegTech La spinta per il nuovo mercato finanziario, 5. *www.pwc.com/it*
[220] In argomento v. VIANELLI, VALENTI, *RegTech e Modelli 231: uno sguardo al futuro per un'esigenza presente*, in *Giurisprudenza Penale*, 2021, 4 ss.
[221] Nel 2020 è stata registrata una crescita del 54,9% degli investimenti in materia *Regtech*, v. PWC, *RegTech La spinta per il nuovo mercato finanziari*o, 7. www.pwc.com/it
[222]Anche se su scala più ridotta, anche in Italia è riscontrabile un *trend* di crescita in materia.

[223] Dato riportato dal report 2023 del Fintech Discrict di Milano *https://www.fintechdistrict.com/*

particolare quelli di *Risk Assesment*, allo scopo di prevenire i rischi idonei ad arrecare un danno alle aziende sviluppa algoritmi predittivi del rischio grazie all'intelligenza artificiale.

La seconda è un'azienda nata a Roma nel 2010 che si occupa nello specifico di predisporre meccanismi basati sulle nuove tecnologie per prevenire il reato di frode. Quest'ultima, avvalendosi dell'intelligenza artificiale, è in grado di raccogliere e analizzare in tempo reale una mole enorme di dati ed informazioni così da garantire un presidio antifrode e antiriciclaggio[224].

3. L'utilizzo dell'IA nell'*Internal Investigation*

Con la locuzione *Internal investigation* si fa riferimento all'insieme delle operazioni di controllo poste in essere dall'ente con l'obiettivo di accertare la presenza nel tessuto aziendale di possibili violazioni di legge e regolamenti interni idonee a configurare una responsabilità civile, penale e amministrativa o, più semplicemente, un danno reputazionale in capo ai soggetti che a qualunque titolo operano nella società[225]. In aggiunta, in presenza di reati integrati da apicali o sottoposti appartenenti all'elenco tassativo di fattispecie criminose contemplate dagli articoli 24 ss. del d.lgs 231/2001, risulta possibile ascrivere un *tertium genus* di responsabilità in capo alla persona giuridica.

Quello dell'investigazione interna rappresenta uno strumento che radica le proprie origini nell'ordinamento anglo-americano. A partire dagli anni dell'industrializzazione, infatti, sono stati ha introdotto i c.d. *compliance programs*, vale a dire programmi orientati ad incentivare la

[224] Cfr. ELLENA, *RegTech: quali sono le aziende attive in Italia*, in *Money*, 2023, *https://www.money.it/regtech-quali-sono-le-aziende-attive-in-italia*

[225] Sul punto v. NICOLICCHIA, *Corporate Internal Investigations e diritti dell'imputato del reato presupposto nell'ambito della responsabilità «penale» degli enti: alcuni rilievi sulla base della «lezione americana»*", in *Riv. Trim. Dir. Pen. Ec*., 2014, 781 ss.; NIETO, *Internal Investigations, Whistle-Blowing, and Cooperation: The Struggle for Information in the Criminal Process*, in MANACORDA, CENTONZE, FORTI (eds.), *Preventing Corporate Corruption. The Anti-Bribery Compliance Model*, Londra, 2014, 69 ss; MANCUSO, *Le investigazioni interne nel sistema processuale italiano: tra vuoto normativo e prassi applicative incerte*, in Convegno Associazione dei componenti degli Organismo di Vigilanza – aodv231, 2018; D'ACQUARONE, ROSCINI-VITALI, *L'investigazione interna nel procedimento a carico dell'ente: alcuni spunti per l'integrazione del modello di organizzazione di gestione*, in *La resp amm. soc. e enti*, 2020, 1, 317

compliance delle imprese attraverso l'istaurazione di forme di collaborazione con le pubbliche autorità in cambi di vantaggi per l'ente. È in questo contesto che si diffondono le prime operazioni di investigazione interna: le imprese, in modo particolare le multinazionali caratterizzate da più sedi[226], hanno deciso di acquisire informazioni ed accertare le dinamiche che hanno condotto alla commissione di un illecito nel tessuto aziendale, al fine di collaborare con gli organi inquirenti e conseguire i relativi benefici[227] quali, in particolare, il differimento del procedimento penale in attuazione di un *deferred prosecution agreement*, il mancato esercizio dell'azione penale in presenza di un *non prosecution agreement* ovvero la riduzione delle sanzioni pecuniarie in esito all'attività di collaborazione[228].

Come per i modelli organizzativi, la cui predisposizione non rappresenta un obbligo per l'ente ma, tuttalpiù, un onere a cui adempiere in cambio di benefici che si estrinsecano diversamente a seconda dei casi, anche in relazione alle *internal investigations*, non sussiste una norma che attesti l'obbligatorietà delle stesse. L'unico riferimento normativo che attesti, seppur implicitamente, l'esigenza di prevedere controlli interni alla società è rinvenibile nell'art. 2381 cc. Questi ultimi risultano infatti propedeutici all'esercizio dell'attività di valutazione dell'adeguatezza dell'assetto organizzativo, ammnistrativo e contabile della società che costituisce uno dei doveri sussistenti in capo al consiglio di amministrazione, come esplicitato dal comma terzo della disposizione normativa menzionata[229].

---

[226] Cfr. D'ACQUARONE, ROSCINI VITALI, *L'investigazione interna nel procedimento a carico dell'ente*, cit., 2020, 1, 321

[227] Sul punto v. BURTIN, HOULE, *Investigazioni interne: uno sguardo all'esperienza americana*, in CENTONZE, MANTOVANI (a cura di), *La responsabilità "penale" degli enti. Dieci proposte di riforma*, Bologna, 2016, 199.

[228] Cfr. NICOLICCHIA, *Corporate Internal Investigations e diritti dell'imputato del reato presupposto nell'ambito della responsabilità «penale» degli enti*, cit.,783 ss; ARLEN, BUELL, *L'importanza della regolamentazione delle indagini interne nella giustizia negoziate degli enti*, in CENTONZE, GIAVAZZI («a cura di») *Internal Investigations, best practices e istanze di regolamentazione*, Torino, 2021, 8 s.

[229] V. TOMBARI, *Governo Societario, compliance e "indagini interne" nella s.p.a. quotata*, in ROSSI (a cura di), *La corporate compliance: una nuova frontiera per il diritto*, Milano, 2017, 276 ss.

Preso atto della non obbligatorietà delle *internal investogations*, sono molteplici i vantaggi per l'ente che decide di porre in essere le operazioni di investigazione interna. In primo luogo, i controlli interni rivestono un ruolo di fondamentale importanza in un momento precedente alla verificazione della fattispecie criminosa, vale a dire nell'attività di *risk assesment e risk management*. Gli stessi risultano infatti funzionali a misurare, analizzare, gestire e monitorare i rischi, in modo particolare quello di commissione dei reati nel tessuto aziendale, con l'obiettivo ultimo di ridimensionarli notevolmente[230].

Il loro contributo è apprezzabile anche nella fase successiva alla commissione del reato da parte di un apicale o di un sottoposto. Questi ultimi consentono infatti all'ente di ricostruire le dinamiche del fatto, identificare i soggetti coinvolti, comprendere i diversi profili di responsabilità degli stessi, quantificare le conseguenze derivanti dall'illecito, raccogliere il materiale probatorio da fornire ai legali della società e prendere cognizione delle falle organizzative che non hanno impedito la commissione dell'illecito, salvo un'elusione fraudolenta dele stesse[231].

Oltre alla ricostruzione di tutti gli elementi che hanno comportato la verificazione di un reato presupposto nell'ente, *l'internal investigation* consente all'ente di intervenire con maggiore tempestività[232] nella predisposizione delle condotte riparative e di riorganizzazione *post delictum*, dove il fattore temporale è determinante nella scelta del beneficio da concedere alla persona giuridica alla luce di quanto stabilito dagli articoli 12, 17 e 78 del d.lgs. 231/2001.

---

[230] Così COTTONE, MANTOVANI, *La reazione dell'impresa a fronte di «segnali di allarme» e/o di indagini della magistratura*, in BONELLI, MANTOVANI (a cura di), *Corruzione nazionale e internazionale*, Milano, 2014, 10 s.

[231] Cfr. CATTANEO, *Le indagini interne: presupposti, finalità e aspetti operativi, Atti del Convegno AODV231 – "L'Organismo di Vigilanza tra Indagini Interne e Investigazioni Processuali"*, Milano, 2013, 15.

[232] V. BASSI, MORELLI, *Internal Investigations: uno strumento di monitoraggio e governo del rischio nell'ottica dell'efficacie attuazione del modello organizzativo*, in *La resp. amm. soc. e enti*, 2019, 4, 293.

Illustrati i vantaggi che l'ente ha la possibilità di conseguire attraverso la conduzione di attività di investigazione e controllo interno, è utile esplicitare in cosa consistono concretamente e quali sono le varie fasi in cui si estrinsecano, per poi comprendere in che modo i nuovi paradigmi tecnologici possano rilevarsi un valido supporto alle stesse.

L'opportunità di predisporre un'indagine interna può derivare da una molteplicità di fonti. L'*input* può essere determinato in *primis* dagli organismi indipendenti quali, a titolo esplicativo, l'ANAC, la Consob e la Banca d'Italia, le quali, nell'esercizio dell'attività di ispezione a cui sono preposte, possono richiedere all'ente la documentazione nonché le informazioni che attestino la compliance dello stesso con le normative di settore[233].

L'Occasione di dare il via alle operazioni investigative interne può essere determinata altresì dall'acquisizione di una notizia di reato: in questo secondo caso l'ente verrà spinto a ricostruire le dinamiche del fatto e a identificare i soggetti coinvolti al fine di predisporre la miglior strategia difensiva possibile[234].

Diversamente, la necessità di investigare potrebbe derivare da segnalazioni provenienti dall'Organismo di Vigilanza nell'esercizio delle funzioni a cui è preposto ovvero dagli altri soggetti appartenenti all'organico dell'impresa e addetti alle funzioni di controllo quali ad esempio il responsabile della funzione di *internal audit* e il responsabile degli affari legali.

Infine, la scelta di operare un*'internal investigation* potrebbe scaturire da una segnalazione interna proveniente dai sistemi di *whistleblowing*, vale a dire un canale predisposto dall'ente al fine di consentire ai soggetti che a vario titolo operano nello stesso di segnalare in via del tutto anonima eventuali segnali di rischio, condotte illecite o fattispecie criminose già verificatesi. Si tratta di uno strumento adottato per

[233] Sul punto v. D'ACQUARONE, ROSCINI-VITALI, *L'investigazione interna nel procedimento a carico dell'ente*, cit., 2020, 320.
[234] In argomento sempre D'ACQUARONE, ROSCINI-VITALI, *L'investigazione interna nel procedimento a carico dell'ente*, cit., 2020, 320.

la prima volta nei paesi di *common law* a partire dagli anni '40 del Novecento che, da oltre dieci anni, è oggetto di una specifica disciplina anche nel nostro ordinamento giuridico[235].

Quest'ultimo è stato introdotto per la prima volta nel nostro Paese con la l. n. 90 del 2012 intitolata "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella Pubblica Amministrazione", che all'art. 1, comma 51 ha previsto l'inserimento dell'art. 54-bis nel d. lgs. 30 marzo 2001 n. 65 recante la disciplina organica in merito alla "Tutela del dipendente pubblico che segnala illeciti"[236].

Il meccanismo è stato esteso anche al settore pubblico in virtù della legge n. 179 del 2017 intitolata "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato". La stessa disposizione legislativa ha introdotto nuove regole in materia di *whistleblowing,* in parte emendate a cura dell'ultimo intervento normativo in materia, il d.lgs. 24/2023, che tuttavia ha mantenuto la rilevanza della suddetta pratica anche nella configurazione della responsabilità da reato degli enti in quanto la stessa assurge a requisito di idoneità del modello organizzativo insieme a quelli contemplati dall'art 6 del d.lgs 231/2001, con la conseguente introduzione della possibilità di istituire specifici sistemi di tutela per coloro che operano delle segnalazioni[237].

Quanto già delineato in relazione alle fasi di costruzione di un modello organizzativo può ben essere esteso al tema delle Investigazioni interne. Anche in relazione al tema delle Investigazioni interne è possibile cogliere i benefici derivanti dall'impiego delle nuove tecnologie a supporto delle stesse. A dimostrazione delle opportunità connesse ad una digitalizzazione delle *internal investigations* è utile procedere sulla

[235] L'ultimo intervento normativo sul punto è rappresentato dal d.lgs. 24/2023

[236] L'art. 54-bis del D.lgs. 30 marzo 2001 n. 165 prevede che: «il pubblico dipendente che denuncia all'autorità giudiziaria o alla Corte dei conti, ovvero riferisce al proprio superiore gerarchico condotte illecite di cui è venuto a conoscenza in ragione del proprio rapporto di lavoro, non può essere sanzionato, licenziato o sottoposto ad una misura discriminatoria, diretta o indiretta, avente effetti sulle condizioni di lavoro per motivi collegati direttamente o indirettamente alla denuncia»

[237] V. MORGANTE, FIORINELLI, *Promesse e rischi della compliance penale digitalizzata*, cit., 7.

falsariga di come pocanzi fatto in relazione alle diverse fasi di costruzione di un modello organizzativo, vale a dire delineando gli *step* di cui constano le Investigazioni interne per poi comprendere come i nuovi paradigmi tecnologici possano validamente supportarli e perfezionarli.

Il procedimento di *internal investigation*, da quanto risulta dalle prassi consolidatesi in materia, consta di sette attività principali[238]

Prima fra tutte la fase di *Alert*, la quale consiste nella produzione nonché ricezione da parte dell'OdV di un segnale di allarme volto ad evidenziare la presenza di un'anomalia nel contesto aziendale. L'utilità di questo primo momento di investigazione consiste proprio nella rilevazione di tutti quei comportamenti sospetti in quanto idonei a configurare un rischio di commissione di una fattispecie criminosa. Tale attività di segnalazione iniziale riveste un ruolo di fondamentale importanza poiché se condotta in maniera tempestiva e attendibile, consente all'ente di reagire in tempo e prevenire la verificazione del reato.

È proprio in relazione alle esigenze di rapidità e completezza che si colgono le opportunità connesse all'utilizzo dei nuovi presidi tecnologici in questa fase di segnalazione in modo da automatizzare la fase di *alert*.

Il *tool* che viene in rilievo nello specifico è quello di *real time analytics:* un *software* capace di monitorare in tempo reale lo svolgimento di tutte le attività aziendali nonché inviare segnalazioni tempestive all'organismo di vigilanza in presenza di anomalie o circostanze che destano sospetto[239].

Il secondo *step* da compiere all'interno del processo di investigazioni interne è rappresentato dal *Risk Assesment*[240]: in questa fase la società ha il compito di valutare le segnalazioni ricevute in sede in *Alert*, così da stabilire se avviare la procedura di *internal investigation* vera e propria. Anche in questo secondo caso le nuove tecnologie consentono il raggiungimento di risultati più rapidi e più precisi. È prospettabile in questo secondo caso

[238] In argomento v. FORTUNATO, DI NOCCO, *Corporate Governance. Le fasi e i processi operativi di un'indagine interna o «internal investigation»*, in *Riv. dott. comm*., 2018, 234.

[239]In argomento v. D'AGOSTINO, *Criminal Compliance e nuove tecnologie*, in corso di pubblicazione, 21.

[240] V. FORTUNATO, DI NOCCO, *Corporate Governance. Le fasi e i processi operativi*, 2018, cit., 234.

l'utilizzo di tecniche di *big data analysis,* le quali provvedono dapprima all'analisi dei dati forniti, nel caso di specie le segnalazioni di comportamenti rischiosi e alla luce della stessa suggeriscono all'ente la miglior soluzione da adottare nel caso di specie.

La terza attività propria delle investigazioni interne è rappresentata dal *Planning*, vale a dire il momento in cui l'ente deve programmare nel dettaglio le modalità di svolgimento dell'indagine, stabilire le tempistiche e definire le risorse da impiegare. Predisporre il piano in questione su un supporto digitale consente di rendere lo stesso maggiormente comprensibile nonché meglio condivisibile.

È nel il *Kick-Off* da rintracciare il terzo *step* che connota le operazioni di *internal investigation*. Quest'ultimo consiste nella predisposizione nonché condivisione di un mandato di *internal investigation* che sta ad indicare l'avvio vero e proprio delle indagini. È possibile digitalizzare questo passaggio attraverso la tecnologia *blockchain,* in grado di avviare in automatico una procedura o rendere esecutivo un documento al verificarsi delle condizioni previamente stabilite dalle persone fisiche.

La fase *core* delle indagini interne è rappresentata dall'*Execution*, vale a dire il momento il cui vengono poste in essere le operazioni di ricerca e di analisi della documentazione aziendale, si conducono le interviste e si procede alla valutazione degli elementi di prova ottenuti fino a questo momento. Anche nell'esecuzione di questo *step* appare particolarmente proficuo avvalersi degli algoritmi di *Big Data Analysis,* utili a passare in rassegna in maniera rapida ed efficace i dati da processare, per poi ricavarne delle informazioni utili.

L' *internal investigations* si concludono infine con le ultime due fasi, quella di c.d. *Reporting* e quella di c.d. *Remediation.* La prima consiste nella redazione di un documento riassuntivo che riporti tutti gli esiti delle operazioni di indagine poste in essere, relazione che va successivamente trasmessa al *Managment* il quale è deputato a dare concreta attuazione ai provvedimenti necessari alla luce di quanto emerso dal documento finale.

La seconda e ultima fase delle indagini interne prende il nome di è

deputata all'adozione di misure correttive man mano che le operazioni di controllo procedono. Appare utile digitalizzare anche queste ultime fasi e supportare le stesse attraverso gli algoritmi di AI per le stesse ragioni prospettate in relazione agli step precedenti.

Se finora l'analisi si è concertata sui profili sostanziali che interessano il tema delle Investigazioni interne, è utile dedicare dei brevi cenni altresì al rapporto che intercorre tra le stesse e l'instaurazione di un procedimento a carico dell'ente volto ad accertare la responsabilità dello stesso ai sensi del d. lgs. n. 231 del 2001.

La seconda finalità perseguibile dalle *internal investigations* è quella c.d. processuale, queste ultime consentono infatti all'ente *in primis* di acquisire tutte le informazioni utili alla ricostruzione dei fatti oggetto dell'ipotesi accusatoria, di raccogliere l'insieme degli elementi volti ad accertare i diversi profili di responsabilità ascrivibili alle persone fisiche nonché di acquisire gli elementi che poi fonderanno la strategia difensiva fatta valere in udienza [241].

Le *internal investigations*, alla luce degli elementi ottenibili attraverso le stesse, conferiscono altresì la possibilità alle imprese di scegliere se collaborare o meno con l' autorità inquirente nonché, l'opportunità di conseguire i numerosi incentivi contemplati dal d.lgs. 231/2001. L'ente, infatti, per poter giovare dei benefici previsti dal decreto legislativo, deve in primo luogo dimostrare l' efficace funzionamento del sistema di controlli interni e, in ogni caso, incarnare un atteggiamento proattivo nella risposta all'illecito.

L'aver predisposto delle indagini interne consente all'ente di dimostrare il comportamento virtuoso tenuto, rimuovendo qualsivoglia sospetto in merito alla sua previa conoscenza o tolleranza delle condotte illecite tenute da apicali o sottoposti in azienda, e dimostrando altresì di non avervi cooperato.

[241] Sul punto v. MANCUSO, *Le investigazioni interne nel procedimento a carico dell'ente*, in CASTRONUOVO, DE SIMONE, GINEVRA, LIONZO, NEGRI, VARRASO (a cura di), *Compliance. Responsabilità da reato degli enti collettivi*, Milano, 2019, 1934

La predisposizione di investigazioni interne rapprese una scelta proficua anche nell'ipotesi in cui l'azienda voglia adottare delle condotte riparatorie *post delictum*, ai sensi degli artt. 12 e 17 d.lgs. n. 231/2001, la realizzazione delle quali, nel caso sia instaurato il giudizio per la verifica della colpevolezza dell'ente, consentirà l'accesso a benefici sanzionatori, quali l'esclusione delle sanzioni interdittive oppure l'attenuazione delle sanzioni pecuniarie o procedurali[242].

Anche per il potenziamento delle *internal investigations* orientate a perseguire questa seconda finalità processuale, appare opportuno sfruttare i nuovi paradigmi tecnologici. Questi ultimi, infatti, per le stesse ragioni enumerate quando si è trattato dei rilievi sostanziali, andrebbero a perfezionare le stesse in termini di completezza, efficacia e rapidità.

Se alle nuove tecnologie va attribuito il merito di apportare molteplici benefici alla conduzione delle indagini interne, non si può fare a meno di osservare che la migliorata pervasività delle stesse comporta altresì l'intensificazione del già rilevante divario che sussiste tra l'ente e la persona fisica quanto agli strumenti di difesa a disposizione in presenza di una notizia *criminis*.

Lo squilibrio delle forze in campo è evidente sotto molteplici profili[243]. Primo fra tutti la diversa disponibilità economica in capo alla persona giuridica, da prassi notevolmente maggiore rispetto a quella del singolo individuo coinvolto. Un potere di spesa capace di condizionare la scelta del difensore a cui affidarsi nonchè la predisposizione della strategia difensiva orientata a dimostrate la propria estraneità al fatto criminoso.

Il secondo luogo, l'interesse che muove le diverse parti coinvolte. L'ente, dimostrando la responsabilità della sola persona fisica, ha la possibilità di conseguire l'immunità o, comunque i notevoli sconti di pena contemplati dal d.lgs. 231/2001, è per queste ragioni che adotterà le migliori

[242] In argomento v. MANCUSO, *Le investigazioni interne nel procedimento a carico dell'ente,* cit, 1935 ss

[243] Sul punto v. NICOLICCHIA, *Corporate Internal Investigations e diritti dell'imputato del reato presupposto nell'ambito della responsabilità «penale» degli enti,* cit.,783 ss

strategie possibili volt ad attestare la sua estraneità dal reato e il solo coinvolgimento dell'apicale o del sottoposto, a seconda del caso specifico.

Le circostanze appena delineate risultano idonee a minare il rispetto delle garanzie fondamentali riconosciute in capo ad ogni individuo indagato o imputato da parte degli articoli 391 bis ss. del codice di procedura penale, un compendio di disposizioni funzionali a stabilire i soggetti legittimati, le modalità di conduzione delle indagini difensive e le circostanze che devono sussistere affinché i risultati conseguiti in questa fase siano utilizzabili a processo.

In materia di *internal investigations*, infatti, manca una disciplina simile a quella in vigore in materia di indagini difensive che preveda regole specifiche nell'esercizio delle stesse, lacuna idonea a minare il diritto fondamentale alla difesa spettante alla generalità dei consociati in tutte le sue declinazioni.

Per mettere fine alla problematica poc'anzi sollevata, si auspica un intervento legislativo volto a disciplinare nel dettaglio le indagini interne all'ente e ad estendere l'obbligo di rispettare le garanzie difensive enumerate dal codice di procedura penale anche a queste ultime. In questa direzione, parte della dottrina[244] suggerisce di introdurre nel nostro ordinamento una specifica previsione, sulla falsariga del già vigente art. 220 disp. att. cpp., volta a sancire il dovere di rispettare i diritti ascrivibili al singolo secondo quanto previsto dal codice di rito anche per la persona giuridica che intende condurre l'insieme delle indagini interne all'azienda, assicurando, in questo modo, che le prerogative difensive generalmente riconosciuti vengano tutelate al meglio.

4. Profili *de iure condendo*: l'introduzione di misure premiali per l'ente che adotta misure di *digital criminal compliance*

Una delle questioni più problematiche che si pongono in relazione all'approccio delineato dal d.lgs. 231/2001 fa riferimento alla scarsità di

[244] Cfr. NICOLICCHIA, *Corporate Internal Investigations e diritti dell'imputato del reato presupposto nell'ambito della responsabilità «penale» degli enti,* cit.,786 ss.

pronunce giudiziali che attestino l'idoneità del modello organizzativo, tale da garantire l'esonero integrale della responsabilità per l'ente[245]. Questa circostanza rappresenta un fallimento della 231 in quanto disattende le prospettive premiali che spetterebbero alla persona giuridica che si sia adoperata nella predisposizione dell'insieme dei presidi organizzativi[246].

L'esclusione della responsabilità dell'ente è stabilita qualora si provi che quest'ultimo abbia adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi[247]. È pertanto nell'accertamento della sussistenza dei caratteri dell'adozione del modello, della sua efficace attuazione e dell'idoneità dello stesso che si dovrebbe fondare la valutazione giudiziale volta ad escludere la responsabilità in capo all'impresa, dove il ruolo preponderante è rivestito dal requisito dell'idoneità, posto che gli altri due risultano elementi che si limitano ad integrare lo stesso[248].

Un primo elemento preliminare e imprescindibile che deve sussistere al fine di ottenere un giudizio positivo circa l'idoneità del MOG è rappresentato dell'adozione, carattere che fa riferimento all'esistenza concreta dell'insieme dei presidi organizzativi che compongono il modello. In aggiunta a quest'ultimo, autorevole dottrina è dell'idea che occorra la presenza tre ulteriori requisiti fondamentali quali l'adeguatezza, l'effettività e l'efficienza.

Quanto al primo, se alcuni autori lo considerano un attributo sinonimo di idoneità[249], altri ritengono più opportuno scindere i due sostantivi a livello di significato: l'adeguatezza si sostanzia in un'attitudine

---

[245] In argomento v. SEVERINO, *Il sistema di responsabilità degli enti ex d.lgs. n. 231/2001: alcuni problemi aperti*, in CENTONZE, MANTOVANI (eds.), *La responsabilità «penale» degli enti. Dieci proposte di riforma*, Bologna, 2016, 73 ss.; MANACORDA, *L'idoneità preventiva dei modelli di organizzazione*, cit., 100 ss; GULLO, *I modelli organizzativi*, in LATTANZI, SEVERINO (a cura di), *Responsabilità da reato*, vol. I, cit., 267 ss.; MANACORDA, *L'idoneità preventiva dei modelli di organizzazione*, cit.,

[246] Sul punto v. GULLO, *I modelli organizzativi*, in LATTANZI, SEVERINO (a cura di), *Responsabilità da reato*, vol. I, cit., 268.

[247] Ex art 6, co. 1, 231/2001

[248] Cfr. GULLO, *I modelli organizzativi*, in LATTANZI, SEVERINO (a cura di), *Responsabilità da reato*, vol. I, cit., 252.

[249] È di quest'idea MANACORDA, *L'idoneità preventiva dei modelli di organizzazione*, cit., 71.

solo astratta del modello a prevenire i reati della stessa specie di quello posto in essere poiché progettato tenendo delle peculiarità concrete dell'ente e della realtà imprenditoriale in cui opera[250]. Da sola pertanto non è sufficiente a fondare il giudizio positivo poiché occorre l'accertamento ulteriore circa l'attuazione concreta del modello e la sua efficienza, l'idoneità rappresenta quindi una sorta di *upgrade* dell'adeguatezza perché è l'esito di queste verifiche ulteriori.

Per effettività del modello si fa riferimento alla sua reale attuazione così da non restare solo un progetto su carta ma che si sostanzi in presidi organizzativi concreti. Questo requisito è volto a scongiurare la cosiddetta "*cosmetic compliance*"[251] ovvero di un'adozione solo formale delle indicazioni fornite dal d.lgs. 231/2001 volte a scongiurare una responsabilità in capo all'ente[252].

In ultimo, il connotato dell'efficacia implica la capacità del modello di adattarsi ai diversi mutamenti organizzativi dell'ente, fisiologici nel tempo, attraverso la predisposizione di una procedura utile a conseguire un costante aggiornamento dello stesso. Per concludere: l'idoneità preventiva di un modello organizzativo si sostanza nella sua capacità di prevenire il fatto-reato[253].

La quasi radicale assenza di pronunce giudiziali volte ad attestare l'idoneità di un modello organizzativo alla luce dei requisiti sopra delineati, eccezion fatta per le sentenze di merito e l'ultima pronuncia della Corte di

---

[250] Espressione utile a rendere bene il significato di adeguatezza è quella del modello "*tailor made*" ovvero "cucito addosso all'ente", così GULLO, *I modelli organizzativi*, in LATTANZI, SEVERINO (a cura di), *Responsabilità da reato*, vol. I, cit., 253; dello stesso avviso MANES, TRIPODI, *L'idoneità del modello organizzativo* in CENTONZE, MANTOVANI (a cura di), *La responsabilità "penale" degli enti. Dieci proposte di riforma*, Bologna, 2016. 138 secondo cui un modello non debba consistere in un manufatto preconfezionato ma una confezione sartoriale, idonea ad adattarsi alle specificità delle singole società.

[251] Espressione utilizzata da LAUFER, *Inautenticità del sistema della responsabilità degli enti e giudizio di colpevolezza*, in CENTONZE, MANTOVANI (a cura di), *La responsabilità "penale" degli enti. Dieci proposte di riforma*, Bologna, 2016. 11.

[252] Laufer evidenzia come spesso gli apicali in un ente tendano a porre in essere pratiche di *moral hazard*, che si traduce in uno scongiurare ogni tipo di responsabilità simulando l'adozione di un modello organizzativo idoneo, comportamento spesso reso possibile da carenze investigative e di accertamento proprie dell'ufficio del pubblico ministero, v. LAUFER, *Inautenticità del sistema della responsabilità degli enti e giudizio di colpevolezza*, in CENTONZE, MANTOVANI (a cura di), *La responsabilità "penale" degli enti. Dieci proposte di riforma*, Bologna, 2016. 11.

[253] Sul punto v. MANES, TRIPODI, *L'idoneità del modello organizzativo*, cit., 138.

Cassazione sulla vicenda Impregilo, sembrerebbe derivare dalla generale tendenza, propria della magistratura giudicante, di omettere una valutazione nel merito e decretare l'inidoneità del MOG per la sola circostanza che si sia verificata una fattispecie criminosa nel tessuto aziendale[254]. La suddetta valutazione andrebbe concretamente posta in essere e non dovrebbe basarsi sulla capacità del modello di impedire in termini assoluti la verificazione di una fattispecie criminosa nel tessuto aziendale ma sull'idoneità dello stesso ad abbassare il rischio di commissione degli stessi[255], come in ultimo precisato dai giudici di legittimità nella sentenza che ha decretato la fine del caso Impregilo.

Nell'ottica di ridimensionare l'ampia discrezionalità di cui gode l'autorità giudiziaria in questo frangente, si è prospettata la creazione di un meccanismo di certificazione del modello che si sostanzia nell'affermazione anticipata circa la sua idoneità volta a garantirgli l'esclusione da ogni forma di responsabilità[256].

Una tale soluzione risulta già presente in alcuni ordinamenti giudiziari di Paesi esteri[257] e nel nostro Paese è stata oggetto di una specifica proposta elaborata da un *team* di studiosi di diritto penale nell'ambito del c.d. progetto Arel. L'idea di predisporre un meccanismo di validazione anticipata sembrerebbe affondare le proprie radici nell'istituto "dell'asseverazione dell'idoneità dell'efficace attuazione dei modelli di organizzazione e gestione della sicurezza" presente in materia di infortuni sul lavoro[258] e come lo stesso prevede che la valutazione preventiva sui modelli venga posta in essere da un comitato di soggetti privati qualificati:

---

[254] In argomento v. GULLO, *I modelli organizzativi*, in LATTANZI, SEVERINO (a cura di), *Responsabilità da reato*, vol. I, cit., 268.
[255] V. MORGANTE, FIORINELLI, *Promesse e rischi della compliance*, cit., 12.
[256] Cfr. MANACORDA, *L'idoneità preventiva dei modelli di organizzazione*, cit., 71.
[257] Manacorda fa riferimento alla novella legislativa cilena in materia di responsabilità penale delle persone giuridiche
[258] all'art. 51, co. 3-bis, d.lgs. n. 81/2008, "gli organismi paritetici (...) su richiesta delle imprese, rilasciano una attestazione dello svolgimento delle attività e dei servizi di supporto al sistema delle imprese, tra cui l'asseverazione della adozione e della efficace attuazione dei modelli di organizzazione e gestione della sicurezza di cui all'articolo 30, della quale gli organi di vigilanza possono tener conto ai fini della programmazione delle proprie attività

professionisti iscritti in un apposito elenco tenuto dal Ministero della Giustizia, previa attestazione da parte del Ministero di una serie di requisiti in capo agli stessi[259].

La proposta poc'anzi illustrata, oltre ad essere stata disattesa dall'esecutivo, è stata oggetto di critiche da parte di autorevole dottrina[260] che ne ha lamentato, in modo particolare, «una sostanziale estromissione del giudice» dal processo di valutazione in merito all'idoneità, con conseguente violazione del principio del libero convincimento del giudice.

Piuttosto che contemplare un meccanismo che attesti aprioristicamente l'idoneità del modello in via preventiva senza che l'autorità giudiziaria possa opporvisi in quale maniera, sembrerebbe opportuno delineare una serie di misure premiali per l'ente che abbia adottato un modello dotato di specifici requisiti. Presupposto fondamentale alla base di questa soluzione è rappresentato dalla positivizzazione da parte del legislatore di una serie di requisiti minimi oggettivi che un modello deve contemplare per ambire ad un giudizio positivo di idoneità, posto che le indicazioni già presenti nel decreto non sono idonee a guidare adeguatamente l'ente nelle attività di realizzazione di un MOG[261]. È in questo frangente che vengono in rilievo le nuove tecnologie di cui è stato ampliamente trattato nel presente contributo. Queste ultime si ritiene debbano essere ricomprese nel *set* di requisiti che si richiede vengano contemplati da un articolo ad hoc del d.lgs. 231/2001 in virtù della loro capacità di garantire una maggiore efficienza ed efficacia dei modelli, funzionale al giudizio ultimo di idoneità.

È nella capacità di prevenire i reati presupposto grazie ad una migliore mappatura del rischio-reato, nel contributo in favore di una maggiore trasparenza e completezza dei protocolli nonché nella funzione di valido supporto per l'OdV nella conduzione dei controlli da rinvenire la motivazioni che dovrebbero spingere il legislatore a contemplare le nuove

[259] Cfr. MANACORDA, *L'idoneità preventiva dei modelli di organizzazione*, cit., 102.
[260] V. PIERGALLINI, *Paradigmatica dell'autocontrollo penale: dalla funzione alla struttura del 'modello organizzativo' ex d. lgs. 231/2001*, in *Cass. pen*., 2013, 862
[261] Si fa riferimento ai requisiti delineati dall'art. 6 co. 2 d.lgs 231/2001 di cui viene offerta un'analisi dettagliata nei paragrafi precedenti del presente contributo.

tecnologie tra i requisiti minimi che ogni modello idoneo dovrebbe rispettare, Al fine di incentivare l'ente ad organizzarsi ex ante e non solo in un momento successivo alla verificazione della fattispecie criminosa come tendono a fare gran parte delle PMI, si potrebbero prospettare delle misure premiali preventive per l'ente che sin da subito sceglie di adottare un modello organizzativo in *compliance* con le disposizioni legislative in vigore e nel rispetto dei nuovi requisiti oggetto di auspicabile riforma.

Benefici che potrebbero variamente modularsi, fermo restando che un giudizio in merito all'esclusione da ogni forma di responsabilità dovrebbe restare di competenza della sola autorità giudiziaria.

CAPITOLO III

RISCHI E ZONE D'OMBRA DELLA *DIGITAL CRIMINAL COMPLIANCE*

1. Problematiche ontologiche dell'IA

A questo punto della trattazione, appaiono evidenti i vantaggi connessi all'utilizzo di algoritmi di IA a supporto della *compliance* dell'ente in termini di riduzione del costo delle attività, maggiore rapidità e completezza nell'analisi dei dati, migliore conformità con la normativa in vigore e più efficace contrasto ai reati informatici: tutti fattori capaci di incrementare le possibilità che un modello organizzativo sia passibile di una valutazione positiva di idoneità da parte dell'autorità giudiziaria, giudizio che risulta essere propedeutico all'esenzione da responsabilità per la persona giuridica coinvolta.

Per non incorrere nella c.d. «fallacia dell'automazione»[1] e rinnegare un approccio superficiale alla materia, è necessario soffermarsi in questa fase sul «lato oscuro»[2] della *digital criminal compliance*, delineando i rischi, le zone d'ombra e le questioni giuridiche connesse al fenomeno le quali costituiscono il vero e proprio «prezzo da pagare delle promesse dell'IA»[3]. Una prima questione meritevole di essere approfondita attiene alle problematiche ontologiche dell'intelligenza artificiale, vale a dire quelle caratteristiche intrinseche ai *software* che rendono questi ultimi generatori di rischi e di violazioni delle norme in vigore. L'analisi andrà in un secondo momento a concentrarsi su due questioni problematiche principali: quella della qualità nonché attendibilità dei *big data*, i quali costituiscono gli *input* indispensabili per il funzionamento degli algoritmi intelligenti e quella

[1] Espressione che indica la «fiducia che gli esseri umani tendono a riporre, in modo inconscio e irrazionale, nelle tecnologie, ritenute oggettive e meritevoli di fiducia per il solo fatto di … essere tecnologie» v. COMOGLIO, *Prefazione*, in NIEVA, FENOLL, *Intelligenza artificiale e processo*, 2018, trad. it., Torino, 2019, X-XI; PANATTONI, *Ai and criminal law: the myth of 'control' in a data-driven society*, in VERMEULEN, PERSAK, RECCHIA (a cura di), *Artificial Intelligence, Big Data and Automated Decision-Making in Criminal Justice*, in *RIDP*, 2021, 133.

[2] Cfr. SABIA, *Artificial intelligence and environmental criminal Compliance,* in ESPINOZA DE LOS MONTEROS DE LA PARRA, GULLO, MAZZACUVA (*a cura di*), *The Criminal Law Protection*, cit., 185.

[3] Sul punto v. BURCHARD, *L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società*, in *RIDPP*, 2020, 32.

dell'opacità degli algoritmi di intelligenza artificiale in tutte le sue declinazioni.

Gli algoritmi di intelligenza artificiale se, da un lato, sono apprezzabili per le capacità computazionali che detengono e per la rapidità e l'accuratezza con cui consentono di pervenire ad un risultato, dall'altro, non sono esenti da inesattezze e pregiudizi, meglio noti come *bias,* idonei ad inficiare l'attendibilità degli *output* prodotti dal *tool* e la correttezza dei calcoli posti in essere dallo stesso[4].

Una prima tipologia di *bias* in cui incorre l'intelligenza artificiale si sostanzia nella mancata neutralità dell'algoritmo. Quest'ultimo, infatti, anche se considerato dalla generalità dei consociati come un prodotto tecnologico svincolato da ogni influenza etica, in realtà ricomprende a livello strutturale sia i valori propri di un determinato contesto che i pregiudizi di cui è affetta la realtà circostante[5]. A questa conclusione si giunge alla luce di una duplice circostanza. La prima riguarda gli *input* di cui si serve il *tool*, vale a dire dati ed informazioni che non sempre risultano qualitativamente validi e idonei a rappresentare oggettivamente il contesto oggetto di analisi[6]. La seconda fa riferimento alle diverse modalità di *training* con cui l'algoritmo impara e perfeziona il suo operato[7], le quali consistono in più delle volte nell'osservazione prima e nell'emulazione poi delle scelte operate dalle persone fisiche nella realtà, decisioni mai neutre ma sempre connotate da una base valoriale ben precisa.

Un ulteriore elemento volto ad inficiare l'esattezza dell'analisi condotta dal *software* e, di conseguenza, i risultati a conclusione della stessa, è rappresentato dal c.d. *bias* del *bias*[8], vale a dire dall'insieme delle opinioni e dei pregiudizi che, più o meno inconsciamente, appartengono alla persona

[4] In argomento v. NISCO, *Riflessi della compliance digitale in ambito 231*, in *Sist. pen*., 2022, 11.
[55] Sul punto v. BAMBERGER, *Tecnologies of compliance: risk and regulation in a digital age*, in *Texas law review*, 2010, 707.
[6] Cfr. SABIA, *Artificial intelligence and environmental criminal Compliance,* in ESPINOZA DE LOS MONTEROS DE LA PARRA, GULLO, MAZZACUVA (a cura di), *The Criminal Law Protection*, cit., 185; UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano*, cit., 78.
[7] Per un approfondimento sul punto si rimanda al primo capitolo del presente contributo
[8] v. TREZZA, *L'Intelligenza Artificiale come ausilio alla standardizzazione del modello 231,* cit., 3.

fisica a cui è demandata la creazione della macchina "intelligente". La struttura dell'algoritmo quindi, per quanto il programmatore si sforzi di essere il più oggettivo e neutrale possibile, risentirà inevitabilmente delle credenze dello stesso, andando a produrre dei risultati soggettivamente condizionati.

Il terzo *bias* in cui si rischia di incorrere nel momento in cui si scegliere di utilizzare o paradigmi di intelligenza artificiale non riguarda, a differenza dei primi due, l'ossatura dell'algoritmo ma fa riferimento alla concezione che le persone fisiche hanno dell'IA nonché all'approccio che le stesse riservano all'*output* prodotto dalla macchina. Il fenomeno che viene a configurarsi nel caso di specie prende il nome di *math washing* e consiste nella tendenza a considerare qualsiasi *software* che si avvalga di dati e numeri per rappresentare la realtà complessa come oggettivo, attendibile ed indipendente, anche quando di fatto non incarna i suddetti connotati[9]. Ciò che ne consegue è un atteggiamento scarsamente scrupoloso da parte delle intelligenze umane, le quali risultano solite omettere qualsiasi operazione di verifica sulle operazioni realizzate dal *tool* o confronto sui risultati prodotti dalla macchina per via della cieca fiducia che ripongono nella tecnologia che li ha generati, dando quindi per scontato che gli stessi siano esenti da errori, ontologicamente neutri e matematicamente esatti[10].

Le tre incongruenze sopra illustrate risultano idonee a viziare le operazioni di analisi condotte dall'intelligenza artificiale e appaiono ancor più nocive quando gli *output* ai quali giunge l'IA vengono utilizzati per la prevenzione di una fattispecie criminosa sia nell'ambito della polizia predittiva che con riferimento alla *compliance* interna all'ente[11]. Questi ultimi andranno infatti a condizionare in primo luogo le scelte organizzative interne alla persona giuridica, influenzando tutti gli *step* a cui la persona giuridica deve adempiere per la costruzione di un modello organizzativo

[9] Sul punto v. Attualità Parlamento europeo, Quali sono i rischi e i vantaggi dell'intelligenza artificiale, *https://www.europarl.europa.eu/news/it/headlines/society/20200918STO87404/quali-sono-i-rischi-e-i-vantaggi-dell-intelligenza-artificiale*

[10] Cfr. BAMBERGER, *Tecnologies of compliance: risk and regulation in a digital age*, cit., 712 s.; NISCO, *Riflessi della compliance digitale in ambito 231*, cit. 17

[11] In argomento v. NISCO, *Riflessi della compliance digitale in ambito 231*, cit. 17

idoneo, in secondo luogo avranno un impatto sulle scelte economico-produttive dell'ente[12].

Per ovviare gli effetti negativi derivanti dai *bias* che caratterizzano le nuove tecnologie, appare innanzitutto necessario che i soggetti interessati a utilizzare tecniche di intelligenza artificiale a supporto delle diverse attività di impresa prendano consapevolezza dei vizi ontologici dell'IA, superando il sentimento di generale ed incondizionata fiducia nutrita nei confronti dei software "intelligenti". In secondo luogo, risulta condivisibile la soluzione metodologica prospettata da autorevole dottrina.

Quest'ultima consiste nel c.d. «controllo umano significativo»[13] e si estrinseca nell'onere in capo alle persone fisiche di condurre una serie di operazioni di verifica e riscontro sia sul paradigma tecnologico che sui risultati generati dal *tool*. Andrebbe innanzitutto reso noto il *modus operandi* dell'algoritmo, così che non resti di sola conoscibilità del programmatore o dell'ente che se ne avvale, in secondo luogo occorre che il *software* sia sottoposto ad un controllo di qualità tale da accertarne il rischio di commettere errore, è inoltre opportuno tradurre in un linguaggio "naturale" le formule compositive di un algoritmo, così da dare la possibilità anche a chi non detiene particolari conoscenze e competenze tecnologiche di comprenderne la *ratio* e il funzionamento ed infine sarebbe necessario attuare un confronto tra il risultato automatizzato e quello che, a parità di *input*, avrebbe prodotto un umano.

Procedendo in questo modo, si andrebbe sì a beneficiare dell'efficienza e rapidità nelle operazioni di analisi dei *big data* che solo una macchina può garantire data ma pur sempre verificandone l'attendibilità e la pertinenza prima di prendere decisioni sulla base della stessa.

[12] È il caso in cui i risultati automatizzati vengano utilizzati a supporto della due diligence, per un approfondimento sul punto si rimanda al secondo capitolo del presente contributo

[13] Espressione utilizzata da UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, cit., 14 s.

1.1 Qualità e attendibilità dei *big data*

A questo punto della trattazione, è possibile rinvenire in due variabili principali il minimo comun denominatore tra tutti i paradigmi tecnologici passati in rassegna fino a questo momento. Queste ultime si sostanziano nella notevole capacità di calcolo propria degli algoritmi "intelligenti"[14] e nel ruolo di assoluta centralità rivestito dai *big data* in tutte le operazioni poste in essere dalle macchine automatizzate, caratteristiche, queste ultime, che risultano essere propedeutiche ed interdipendenti tra di loro.

I grandi volumi di dati consentono agli algoritmi di svolgere con maggior completezza compiti per i quali sono stati ideati quali l'analisi delle informazioni, l'identificazione di modelli e correlazioni tra le stesse nonché la scelta della miglior soluzione al problema sottoposto[15] e il notevole impatto che gli stessi hanno sull'intelligenza artificiale è altresì testimoniato dalla possibilità che i nuovi *tools* possano essere programmati per imparare dalle informazioni e per perfezionare il modo in cui vengono prese le decisioni.

Alla luce dei suddetti risultati, ne deriva che l'operato delle nuove tecnologie dipenda significativamente dalla qualità e la quantità dei *data* processati e che entrambe le variabili della quantità ed integrità degli stessi comportino un condizionamento notevole su quelli che sono i risultati elaborati dal *software*, meglio noti come *output*[16].

Una prima questione da affrontare nel momento in cui si decide di avvalersi di algoritmi di IA attiene, pertanto, alla qualità e attendibilità dei grandi volumi di dati adoperati, i quali, metaforicamente parlando, costituiscono il vero e proprio "nutrimento" dei *software* di Intelligenza artificiale perché, proprio come il cibo per gli esseri viventi, risultano

[14] Caratteristiche tecniche indispensabili per processare grandi volumi di dati eterogenei tra di loro.
[15] Per un approfondimento in merito al ruolo rivestito dai big data nel vasto universo delle nuove tecnologie si rimanda al paragrafo ad esso dedicato contenuto nel primo capitolo del presente contributo.
[16] V. BIRRITTERI, *Big Data Analytics e compliance anticorruzione*, cit., 289; SABIA, *Artificial intelligence and environmental criminal Compliance*, cit., 184 s.

indispensabili per porre in essere qualunque operazione e consentono di definire l'essenza di chi se ne avvale[17].

Il connotato della qualità può essere definito in una duplice maniera. L'attributo indica, in primo luogo, il grado di utilità che una determinata informazione detiene in relazione all'obiettivo che la macchina deve raggiungere e fa riferimento, in secondo luogo, alla capacità propria di un determinato dato di essere il più rappresentativo possibile della realtà oggetto di analisi[18].

La questione di estrinseca diversamente a seconda che i paradigmi di IA che si avvalgano dei c.d. algoritmi deterministici o che, al contrario, siano costituiti da c.d. algoritmi non deterministici[19]. Se, nel primo caso, sia gli *input* registrati nel sistema che l'insieme delle indicazioni utili a conseguire un determinato *output* sono fornite dal soggetto programmatore *ex ante*, nel secondo caso, le seguenti variabili vengono ricavate autonomamente dal *software*[20], il quale acquisirà le informazioni dal *web* e imparerà di volta in volta come processarle al meglio per generare un risultato soddisfacente[21].

In relazione al primo caso, se, *prima facie*, parrebbero sussistere più garanzie di qualità dei dati in quanto quelli concretamente sottoposti al *software* sono di numero limitato e rappresentano il frutto di un'attività di selezione da parte del programmatore, in realtà la prassi dimostra come le scelte discrezionali della persona fisica comportino i c.d. *bias* dei *bias*, vale a dire errori dovuti a pregiudizi inconsci, idonei a viziare le attività condotte dal *tool* nonché l'*output* generato in conclusione alle stesse.

È con l'obiettivo di fornire una soluzione alla questione pocanzi illustrata che L'Organizzazione internazionale per la standardizzazione (ISO) ha

[17] Si fa riferimento alla massima "Siamo quello che mangiamo" pronunciata dal filosofo tedesco FEUERBACH nel 1950 per recensire il Trattato dell'alimentazione del popolo, opera riconducibile al medico e fisiologo olandese MOLESCHOTT.

[18] Cfr. ROSATI, *La qualità dei dati, caratteristica fondamentale nei progetti di analisi*, in *Bigdata4innovation*, 2021. *https://www.bigdata4innovation.it/data-science/la-qualita-dei-dati-caratteristica-fondamentale-nei-progetti-di-analisi/*

[19] Per un approfondimento sul punto v. AVANZINI, *Decisioni amministrative e algoritmi informatici. Predeterminazione analisi predittiva e nuove forme di intellegibilità*, Napoli, 2020, 3 ss.

[20] Un esempio calzante è rappresentato dalle tecnologie OSTINT le quali operano su fonti aperte

[21] Sul punto v. AVANZINI, *Decisioni amministrative e algoritmi informatici*, cit., 3 ss.

incardinato nel parametro ISO/IEC 25012[22] reso pubblico nel 2008, un vero e proprio modello di qualità dei dati, il quale si estrinseca in una serie di quindici parametri utili per misurare e valutare l'integrità delle informazioni, per attestare il grado di *compliance* degli stessi con la legislazione in vigore nonché per migliorarne la completezza e l'attendibilità generale di questi ultimi.

Le caratteristiche di qualità contemplate dalla norma vengono considerate sotto due diversi punti di vista, quello c.d. «inerente», che fa riferimento all' intrinseco potenziale dei dati di soddisfare esigenze di qualità e rappresentazione e quello c.d. «dipendente dal sistema», quando i connotati di integrità ed attendibilità delle informazioni dipendono da sistema in cui sono impiegati[23].

Il primo indicatore contemplato dal parametro ISO/IEC 25012 è quello della completezza, requisito che fa riferimento sia al numero di dati a disposizione della macchina che alla loro rappresentatività, vale a dire la capacità degli stessi di fotografare in maniera attendibile la realtà circostante oggetto di analisi. Questo paramento si dimostra di notevole importanza in quanto è stato appurato che entrambe la scarsità di informazioni a disposizione del *tool* e l'alta percentuale di valori mancanti comportano la produzione di un *output* parziale, incompleto e fuorviante perché la macchina automatizzata non è messa nelle condizioni di avere un quadro completo dell'ambiente in cui è immesso, simulato o reale che sia.

Seguono i requisiti di accuratezza sia sintattica che semantica dei dati, di attualità, di coerenza in relazione agli altri archivi presenti, e di credibilità, tutte caratteristiche vengono definite «inerenti»[24] in quanto devono appartenere ontologicamente all'informazione da utilizzare, a prescindere dal contesto specifico in cui è inserita o dall'utilizzo che se ne intende fare.

[22] Per maggiori informazioni si rimanda al sito ufficiale dell'Organizzazione internazionale per la standardizzazione *https://www.iso.org/standard/35736.html*
[23] Cfr. NATALE, *La qualità dei dati e la ISO/IEC 25012*, in *U&C n.2*, 2019, 1
[24] Sul punto v. ISO/IEC 25012 disponibile sul sito ufficiale dell'Organizzazione internazionale per la standardizzazione *https://www.iso.org/standard/35736.html*

La norma ISO/1EC 25012 annovera altresì i requisiti di accessibilità, vale a dire della circostanza per cui il dato sia disponibile a tutti, di comprensibilità, connotato che attiene alla chiarezza dell'informazione, di conformità in relazione alle norme vigenti in materia, ma anche di efficienza, di precisione, riservatezza e tracciabilità, caratteristiche che vengono considerate in parte «inerenti», poiché devono essere incarnate dal dato, ma altresì «dipendenti dal sistema» in quanto una buona percentuale delle stesse deriva dalle capacità del sistema *software* e *hardware* in cui sono utilizzate.

lista di connotati volti a valutare la qualità dei dati si conclude riportando quei requisiti esclusivamente "dipendenti dal sistema", quali la disponibilità, portabilità e ripristinabilità i quali fanno riferimento rispettivamente alla possibilità di avvalersi nuovamente dello stesso dato, alla capacità dello stesso di migrare da un sistema all'altro ed infine alla sicurezza dell'ambiente in cui è conservata l'informazione[25].

La norma ISO/1EC 25012 utile a valutare la qualità dei dati quali *input* di ogni paradigma tecnologico, non va considerata autonomamente ma risulta essere complementare ad uno *standard* ulteriore, anch'esso elaborato e reso pubblico dalla stessa Organizzazione per la standardizzazione nel marzo 2011. Quest'ultimo prende il nome di ISO 25010[26] e costituisce il parametro attraverso il quale è possibile attestare la qualità non del dato ma del software, vale a dire del contesto informatico in cui l'informazione è inserita ed utilizzata.

Questa seconda tipologia di *standard* contempla tre diverse declinazioni di qualità, vale a dire quella interna, quella esterna e quella c.d. «in uso». La prima fa riferimento ai connotati strutturali di un determinato *software*, anche definititi come statici in quanto restano invariati al mutare dall'utente che se ne avvale o dall'ambiente circostante in cui operano. La seconda declinazione di qualità guarda invece alle caratteristiche dinamiche del *tool*, che si sostanziano nel diverso comportamento assunto dallo stesso

[25] Cfr. NATALE, *La qualità dei dati e la ISO/IEC 25012*, in *U&C n.2*, 2019, 1 s.
[26] Per un approfondimento sul punto v. ISO 25010 disponibile sul sito ufficiale dell'Organizzazione internazionale per la standardizzazione *https://www.iso.org/standard/35736.html*

a seconda dell'ambiente simulato in cui si trova ad agire. Infine, per qualità d'uso si fa riferimento all'efficacia e all'efficienza dimostrata dal *software* in un contesto non più simulato ma reale nonché al grado di soddisfazione dimostrato persone fisiche che se ne avvalgono.

Allo stesso modo del primo *standard* passato in rassegna, anche l'ISO 25010 contiene un insieme di parametri utili a valutare le tre diverse categorie di qualità, in un numero pari a 8 con riferimento alle prime due e in un numero pari a 5 quanto alla terza ed ultima tipologia.

È nell'idoneità funzionale da rintracciare il primo indicatore appartenente al sottogruppo di caratteristiche riferite alla qualità interna ed esterna del *software*. Quest'ultima implica la capacità del *tool* di adempiere alle funzioni attese in presenza di condizioni fattuali specifiche. L'idoneità funzionale viene suddivisa a sua volta nelle caratteristiche della completezza, correttezza e adeguatezza, che indicano rispettivamente la capacità del software di adempiere a tutte le attività richieste e di soddisfare a pieno gli obiettivi prefissati, l'attendibilità degli *output* prodotti dalla macchina automatizzata ed infine la capacità di adattarsi al meglio a quanto richiesto da un utente in particolare.

Il secondo degli otto parametri passati in rassegna dallo standard ISO è quello della *performance*, che a sua volta valuta le tempistiche delle prestazioni poste in essere dell'algoritmo in relazione alle risorse impiegate in concreto dallo stesso e alle capacità che dimostra nell'utilizzo concreto.

È nella compatibilità da rinvenire il terzo elemento preso in considerazione dallo standard in esame, volto a valutare la capacità del *tool* di adattarsi ai diversi ambienti, sia simulati che reali, il quale viene suddiviso ulteriormente in due caratteristiche principali quali la coesistenza e dell'interoperabilità che si sostanziano nella capacità di coesistere con altri *software* indipendenti in un ambiente comune e di interagire con questi ultimi.

Seguono i connotati dell'usabilità, dell'affidabilità, della sicurezza, della manutenibilità e della portabilità, volti ad indicare rispettivamente la capacità di adeguarsi alle aspettative dell'utente, l'attitudine a comportarsi

concretamente secondo ciò che è stabilito nelle sue specifiche, il grado di protezione dalle minacce esterne dimostrato, la facilità con cui è possibile apportare modifiche al sistema ed infine l'indipendenza dimostrata dal software nei confronti della piattaforma originaria, utile a garantirne l'impiego in sistemi diversi dalla stessa.

Lo standard ISO 25010 si conclude, infine, elencando i cinque parametri volti a valutare la c.d. qualità in uso e quindi a dimostrare il grado di soddisfazione dimostrato dall'utente che si avvale del *software* in esame. Questi ultimi sono l'*effectivness*, la produttività, la *safety* e la *satisfaction*, connotati che implicano la capacità del *tool* di porre in essere l'azione giusta in relazione al caso specifico, il valore aggiunto apportato dallo stesso, il grado di sicurezza dimostrato dal software ed infine la sua capacità di rendere soddisfatti gli utenti.

In Italia è all'Agenzia per l'Italia Digitale[27] con sede a Roma a cui è demandato il compito di promuovere ed accertare l'applicazione degli standard ISO pocanzi passati in rassegna, parametri che risultano essere stati ricompresi altresì nel Piano triennale per l'Informatica nella Pubblica Amministrazione 2017-2019, in ultimo aggiornato nel 2022. Quest'ultimo dedica l'intero quarto capitolo alle infrastrutture immateriali rimarcando l'importanza di valorizzare il patrimonio informativo della PA in quanto rispettosi dello standard di qualità dei dati per come definito dall'ISO/IEC 25012.

Consapevole dell'esigenza di garantire un buon livello di qualità e attendibilità sia dei *big data* impiegati che dei *software* stessi si dimostra essere il Consiglio d'Europa, il quale, nel dicembre del 2018, ha deciso di annoverare tra i 5 principi fondamentali da rispettare nell'utilizzo dell'intelligenza artificiale incorporati nella Carta Etica Europea quello di qualità e la sicurezza dei paradigmi di IA impiegati nell'analisi di dati e decisioni giudiziarie.

[27] Per maggiori informazioni a riguardo si rimanda al sito ufficiale *www.agid.gov.it*

La Commissione europea per l'efficacia della giustizia[28] ha elaborato tre raccomandazioni principali, funzionali al rispetto del suddetto principio. In primo luogo, si richiede l'utilizzo di fonti certificate e dati intangibili. Risulta, infatti, di fondamentale importanza verificare l'attendibilità della sorgente dalla quale proviene l'informazione nonché l'integrità della stessa. L'intero processo deve essere pertanto tracciabile così da garantire che non abbia avuto luogo alcuna modifica idonea ad alterare il contenuto o il significato della decisione assunta.

In secondo luogo, la Commissione raccomanda che gli algoritmi su cui si basa la decisione giudiziaria vengano custoditi in un ambiente tecnologico sicuro e impenetrabile, nell'ottica di evitare modificazioni e alterazioni improprie degli stessi.

In ultimo, si auspica l'adozione di un approccio multidisciplinare nella creazione di modelli computazionali, così da assicurarne la completezza e la sicurezza: la Commissione consiglia, in particolare, di costituire squadre di progetto miste che vedano la presenza sia di esperti di informatica capaci di progettare modelli di apprendimento automatico che di professionisti del sistema giustizia come giudici, pubblici ministeri, avvocati, e ricercatori nel campo del diritto e delle scienze sociali .

1.2 Opacità: rischio di un effetto "*black box*"

Una seconda questione meritevole di analisi attiene all'opacità degli algoritmi dell'IA, caratteristica che si sostanzia nella mancata trasparenza e comprensibilità sia dei processi decisionali adottati dalla macchina che del risultato in ultimo generato dalla stessa da parte dei soggetti destinatari degli *output* e, in casi particolari, anche dagli esperti che hanno programmato *ab origine* il *tool* "intelligente"[29].

[28] Organismo a cui il Consiglio d'Europa ha conferito il mandato di elaborare una Carta Etica Europea

[29] Di quest'opinione SEVERINO, *Intelligenza artificiale e diritto penale*, in RUFFOLO (a cura di), *Intelligenza artificiale*, cit., 543; UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, cit., 78; SALANITRO, *Intelligenza artificiale e responsabilità: la strategia della commissione europea*, in *Riv. Dir. Civ.*, 2020, 1247; ZUDDAS, *Brevi note sulla trasparenza*

Il rischio che un *tool* risulti oscuro alle "intelligenze umane" che se ne avvalgono è direttamente proporzionale al tasso di autonomia e indipendenza incarnati dallo stesso: tanto più la macchina automatizzata è in grado di acquisire *input*, apprendere dalla realtà circostante e perfezionare gli *output* in maniera svincolata rispetto alle persone fisiche, quanto più risulterà difficile per queste ultime comprendere le ragioni sia logiche che tecniche che hanno spinto la tecnologia in questione ad elaborare un determinato risultato[30].

È possibile distinguere fra tre diverse tipologie di opacità, tutte idonee a mettere a repentaglio il principio di trasparenza algoritmica introdotto e tutelato dal Regolamento UE 2016/679, anche conosciuto come GDPR[31], il quale implica l'onere in capo ai soggetti che si avvalgono di una determinata decisione adottata da paradigma tecnologico di spiegare l'*iter* percorso dalla macchina per giungere alla stessa e di fornire una motivazione nel merito, con il conseguente diritto in capo alle persone fisiche destinatarie dell'*output* automatizzato di ricevere le suddette informazioni[32].

Il principio in questione consta in tre prerogative principali che si estrinsecano nella conoscibilità dell'algoritmo, nella significatività dello stesso ed infine nella sua comprensibilità. Quanto al primo aspetto,

---

algoritmica, in *Amministrazione in cammino*, 2020, 10 ss.; LO SAPIO, *La trasparenza sul banco di prova dei modelli algoritmici*, in *Federalismi.it*, 2021, 242 ss.; SALVADORI, *Agenti artificiali, opacità, tecnologica e distribuzione della responsabilità penale*, in *Riv. It. Dir. Proc. Pen*., 2021, 83 ss.

[30] Sul punto v. BORSARI, *Intelligenza artificiale e respinsabilità penale: prime considerazioni*, in *MediaLaws*, 2019, 265; ZUDDAS, *Brevi note sulla trasparenza algoritmica*, cit., 11; GIANNINI, *Artificial Intelligence, human oversight and criminal liability: an european strenght test*, in *Criminalia*, 2021, 4.

[31] In argomento v. AMORE, "*Fairness", "Transparency" e "Accountability" nella protezione dei dati personali*, in *Studium iuris*, 2020, 414 ss.; AMRAM, *The Role of the GDPR in Designing the European Strategy on Artificial Intelligence: Law-Making Potentialities of a Recurrent Synecdoche*, in *Opinio Juris in Comparatione*, 2020, 73 ss.; VIGLIANISI, *Le nuove frontiere dell'intelligenza artificiale ed i potenziali. Rischi per il diritto alla "privacy"*, in *Persona e Mercato*, 2021, 393 ss; SPILLER, *Il diritto di comprendere, il dovere di spiegare. "Explainability" e intelligenza artificiale costituzionalmente orientata (The right to understand, the duty to explain. Explainability and constitutional oriented artificial intelligence)*, in *BioLaw Journal - Rivista di BioDiritto*, 2021, 419 ss; PIZZETTI, *Il sistema normativo di protezione dei trattamenti di dati personali nel quadro europeo e nazionale*, in PIZZETTI (a cura di),*Protezione dei dati personali in Italia tra GDPR e Codice Privacy*, Milano, 2022, 3 ss.

[32] Cfr. ZUDDAS, *Brevi note sulla trasparenza algoritmica*, cit., 1 ss.

quest'ultimo viene considerato come un diritto assoluto che consiste nella pretesa giuridicamente tutelata ad essere informati circa la presenza di un paradigma tecnologico che si avvalga dei dati personali di un singolo per generare un *output*[33] e trova una puntuale disciplina nell'articolo 15 del GDPR, rubricato "Diritto di accesso dell'interessato", il quale, alla lettera h, contempla il diritto spettante a ciascuno di essere informato circa l'esistenza di un processo decisionale automatizzato che utilizzi che si avvalga dei propri dati personali per generare un risultato specifico.

Lo stesso articolo 15 GDPR contempla altresì la seconda componente che caratterizza il diritto alla trasparenza algoritmica, vale a dire quella della significatività dello stesso. L'ultimo periodo del primo comma del suddetto riferimento normativo disciplina, infatti, il diritto in capo al singolo di sapere quanta importanza è stata conferita all'*output* generato dal paradigma tecnologico nell'assunzione di una determinata decisione che lo riguarda, nonché la pretesa di essere informato circa le conseguenze derivanti dal trattamento automatizzato ad esso riferito[34].

Essere edotti sul ruolo rivestito da un paradigma tecnologico nella scelta di una soluzione ben precisa appare funzionale ad accertare se il trattamento[35] automatizzato dei propri dati personali sia rispettoso di quanto disciplinato dall'articolo 22 GDPR[36], disposizione che prevede il diritto di non essere destinatari di una decisione adottata per intero da un *tool* nel caso

[33] In argomento v. SIMONCINI, SUWEIS, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Rivista di filosofia del diritto*, 2019, 98; SASSI, *Gli algoritmi nelle decisioni pubbliche tra trasparenza e responsabilità*, in *Analisi Giuridica dell'Economia*, 2019, 109 ss.

[34] V. ZUDDAS, *Brevi note sulla trasparenza algoritmica*, cit., 5 s.

[35] L'articolo 4 del GDPR definisce il trattamento come "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione"

[36] Sul punto v. PIZZETTI, *Il procedimento italiano di adeguamento al GDRP e la struttura del Codice novellato*, in PIZZETTI (a cura di), *Protezione dei dati personali in Italia tra GDPR e codice novellato*, Milano, 2022, 63 ss.

in cui la stessa sia idonea a produrre conseguenze sulla propria sfera giuridica soggettiva e ad avere un impatto rilevante sulla propria persona[37].

L'articolo 22 GDPR vieta, pertanto, che una decisione sia totalmente automatizzata, richiedendo la sussistenza di un intervento umano minimo a garanzia dell'attendibilità della soluzione offerta dalla tecnologia. Questa prerogativa subisce una serie di limitazioni elencate nel secondo comma del medesimo articolo quali la sussistenza di un'autorizzazione ad avvalersi del trattamento conferita dall'Unione Europea o da uno Stato membro volta ad ammettere il ricorso ad una procedura di trattamento dei dati personali interamente rimessa alla macchina per perseguire finalità di interesse pubblico, la circostanza per cui la decisione automatizzata sia necessaria per la conclusione o per l'esecuzione di un contratto tra l'interessato e il titolare del trattamento ed infine la presenza di un esplicito consenso da parte della persona fisica coinvolta dal procedimento tecnologico[38]. Infine, l'articolo 22 riconosce ai soggetti interessati dal trattamento automatizzato il diritto di «esprimere la propria opinione e di contestare la decisione»[39], facoltà che tutta via presuppone una conoscenza dei meccanismi impiegati dal *tool* per generare una determinata decisione, la quale risulta a sua volta minata dal connotato dell'opacità il quale rende incomprensibile i suddetti passaggi tecnici e logici.

Il terzo e ultimo profilo che connota il principio di trasparenza algoritmica attiene alla comprensibilità dell'algoritmo. Quest'ultimo si sostanzia nel diritto in capo all'interessato di venire a conoscenza non solo dell'esistenza di un trattamento automatizzato dei suoi dati personali ma di come quest'ultimo si realizzi in concreto[40] con il conseguente onere in capo all'utilizzatore dell'*output* automatico di fornire l'insieme delle informazioni idonee ad illustrate ad un soggetto il più delle volte estraneo al mondo delle nuove tecnologie la "logica" utilizzata dal *tool*.

---

[37] Cfr. ZUDDAS, *Brevi note sulla trasparenza algoritmica*, cit., 6; NISCO, *Riflessi della compliance digitale in ambito 231*, cit., 7.
[38] Sul punto v. PALMIRANI, *Big Data e conoscenza*, in *Riv. filos. dir*., 2020, 73 ss
[39] V. art. 22, co. 3 GDPR
[40] Il diritto alla comprensibilità dell'algoritmo è contemplato dall'art. 15 GDPR

Le suddette indicazioni devono essere fornite in modo chiaro e preciso[41], vale a dire in una forma «concisa, trasparente, intelligibile, facilmente accessibile e con un linguaggio semplice e chiaro», come ha premura di specificare l'art. 12 GDPR rubricato «Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato» e che conferisce altresì la possibilità di avvalersi di icone standardizzate in favore della chiarezza espositiva.

Una volta illustrato il principio di trasparenza algoritmica nella sua triplice accezione, è utile passare in rassegna le tre diverse declinazioni di opacità idonee ad arrecare una violazione dello stesso. La prima tipologia prende il nome di «opacità tecnica», espressione utilizzata per indicare le difficoltà riscontrate dai non addetti ai lavori nel comprendere sia l'algoritmo nei suoi elementi essenziali, che il processo interno allo stesso che ha portato a generare una determinata soluzione[42]. I nuovi paradigmi tecnologici costano infatti di algoritmi, nodi, modelli e strutture così articolate che richiedono conoscenze nonché competenze tecniche specifiche per essere capiti e per saperne giustificare il modo di operare, prerogative il più delle volte detenute dai soli esperti di tecnologie.

L'elemento di oscurità tecnica più evidente attiene al lessico utilizzato dalla macchina, il quale presenta notevoli profili di diversità con quello "naturale" di cui si avvalgono le persone fisiche nella vita di tutti i giorni. Quest'ultimo viene infatti a configurarsi come un linguaggio tecnico in quanto composto da codici e cifre, il quale può risultare criptico e privo di significato per la generalità dei consociati a cui mancano le conoscenze tecnologiche utili alla sua comprensione[43].

La seconda declinazione di opacità prende il nome di opacità intrinseca. Quest'ultima risulta essere un connotato ontologico e strutturale proprio di quei sistemi di IA capaci di apprendere e generare *output* in totale autonomia, senza che il soggetto che ha provveduto a programmarli riesca a comprendere a pieno l'operato degli stessi e le motivazioni che hanno

[41] Secondo quanto previsto nel considerando n. 39 del Regolamento UE 2016/679 (GDPR)
[42] Cfr. ZUDDAS, *Brevi note sulla trasparenza algoritmica*, cit., 10.
[43] Sul punto v. LO SAPIO, *La trasparenza sul banco di prova dei modelli algoritmici*, cit., 243 s.

spinto la macchina a produrre una determinata soluzione piuttosto che un'altra[44]. È il caso dei *software* che si basano sul *macchine learning* o, con profili di ancora maggiore evidenza, su tecniche di *deep learning*. I *tools* in questione nascono proprio come *black boxes*, vale a dire come scatole oscure e quindi impenetrabili e incomprensibili. Questi ultimi, infatti, operano secondo una logia deduttiva in quanto il sistema "impara" a partire da dati solitamente raccolti dal web e progredisce in totale autonomia, con la conseguenza che anche l'integrale rivelazione del codice sorgente potrebbe non determinare la piena comprensibilità del modo di operare della macchina, che spesso è ignota agli stessi programmatori[45].

La terza ed ultima tipologia di opacità è stata definita con l'attributo «giuridica»[46]. Quest'ultima, a differenza di quella tecnica e di quella intrinseca che fanno riferimento a caratteristiche oggettive proprie dei nuovi paradigmi tecnologici, rinviene la propria *ratio* in una serie di prerogative giuridiche vantate dai soggetti "ideatori" di un algoritmo che si basano, *in primis*, sulla tipologia di dati utilizzati all'interno del trattamento automatizzato, in secondo luogo, sulla sussistenza di un diritto di proprietà intellettuale o industriale vantato dagli stessi sui *software* di IA impegnati.

Quanto al primo profilo, è bene chiarire che il diritto alla trasparenza algoritmica contemplato dal GDPR ha ad oggetto il trattamento dei soli dati personali, vale a dire quelle informazioni idonee ad identificare o a rendere identificabile una persona fisica in quanto hanno ad oggetto caratteristiche, convinzioni, pensiero politico, stato di salute, situazione economica e così via[47]. Ne consegue, per contro, la possibilità di utilizzare liberamente i dati

---

[44] In argomento v. BORSARI, *Intelligenza artificiale e responsabilità penale: prime considerazioni*, in *MediaLaws*, 2019, 265; ZUDDAS, *Brevi note sulla trasparenza algoritmica*, cit., 11; GIANNINI, *Artificial Intelligence, human oversight and criminal liability: an european strenght test*, in *Criminalia*, 2021, 4.

[45] Cfr. ZUDDAS, *Brevi note sulla trasparenza algoritmica*, cit., 11.

[46] V. LO SAPIO, *La trasparenza sul banco di prova dei modelli algoritmici*, cit., 245.

[47] La seguente definizione deriva dall'articolo 4 GDPR in virtù del quale è considerabile «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile con particolare riferimento a nome, numero di identificazione, dati relativi all'ubicazione, identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale; La stessa risulta essere condivisa altresì dal Garante Privacy *https://www.garanteprivacy.it/home/diritti/cosa-intendiamo-per-dati-personali*

che non ricadono nella definizione di dato personale[48], senza il bisogno di osservare gli oneri previsti dalla disciplina europea in materia.

In merito al secondo profilo, è possibile affermare che sussista un diritto in capo al programmatore di un *software* o ad un ente privato che si avvale dello stesso di non dichiarare gli elementi tecnici che caratterizzano gli algoritmi nonché il loro modo di funzionare in virtù dei diritti di proprietà intellettuale o industriale che vantano sugli stessi. Nel caso di specie viene pertanto a configurarsi un vero e proprio conflitto di interessi tra i soggetti privati che ricavano una convenienza di carattere economico e commerciale dal mantenere segreti sia i codici sorgente che il *modus operandi* di un *tool*, e il diritto in capo all'interessato di ottenere una spiegazione in merito all'*iter* automatizzato che ha condotto ad una determinata decisione nonché a ricevere una motivazione nel merito della stessa.

La questione è stata affrontata dalla Carta Etica europea la quale, nel commentare il principio di trasparenza contenuto nella stessa, prospetta una soluzione che non si presta a dubbi interpretativi: si raccomanda, infatti, una completa trasparenza in merito agli elementi tecnici che connotano un *tool*, implementata da una relazione volta ad illustrare il funzionamento del processo computazionale in un linguaggio chiaro ed accessibile a tutti, attestando in questo modo la prevalenza del quarto principio contemplato sul diritto alla segretezza vantato dai titolari di un diritto di proprietà intellettuale o industriale[49].

Il diritto alla conoscibilità, significatività e comprensibilità di un algoritmo appare tanto più meritevoli di tutela quando i nuovi paradigmi tecnologici assurgono alla funzione di supporto per i soggetti pubblici nell'assunzione di decisioni in ambito giudiziario ed amministrativo. Nel primo caso verrebbe infatti a configurarsi una violazione dell'obbligo di motivazione dei provvedimenti giurisdizionali sancito dall'articolo 111 della Costituzione e, di conseguenza, del più generale diritto di difesa contemplato dall'articolo 24 della Carta Costituzionale, mentre nella

[48] Si fa riferimento ai c.d. dati generici
[49] Sul tema v. QUATTROCOLO, *Intelligenza artificiale e giustizia*, cit., 8.

seconda situazione sussiste il rischio che si incorra in una violazione dell'obbligo di motivazione dei provvedimenti amministrativi previsto dall' articolo 3 della legge 241 del 1990.

Il connotato dell'opacità di un *software* di intelligenza artificiale spiega i propri effetti negativi anche nel caso in cui i nuovi paradigmi tecnologici vengano utilizzati da un ente privato nella conduzione delle operazioni di *compliance*. È interesse primario della persona giuridica, infatti, comprendere a pieno il processo che ha portato una macchina ad effettuare una determinata scelta o a generare un *output* specifico, il quale andrà a condizionare le scelte economiche ed organizzative dell'ente.

Accettare passivamente un risultato automatizzato ed implementarlo nella propria impresa senza averne compreso la *ratio* e senza averne appurato l'attendibilità rischia di rimettere l'ente in balia di una *software* i cui eventuali output viziati andranno a produrre conseguenze nocive nei confronti dell'ente e delle persone fisiche che se ne sono avvalse.

In aggiunta, l'assenza di trasparenza nell'operato di un *tool* non dà la possibilità di accertare che lo stesso sia rispettoso delle regole volte a regolamentare i processi decisionali automatizzati, prime fra tutte quelle contemplate dal GDPR in materia di protezione dei dati personali, con il rischio di configurazione di profili di responsabilità in capo alle persone fisiche che si sono avvalse dell'output generatore di violazioni[50].

È per la ragioni sopra illustrate che risulta consigliabile avvalersi dei soli *software* che offrano garanzia di trasparenza e di attendibilità, parametri che accertabili confrontando il *tool* con gli standard ISO 25012 e 25012 orientati, rispettivamente, ad attestare la qualità nonché attendibilità dei dati utilizzati e l'attendibilità nonché affidabilità dei *software*. Prediligendo i soli paradigmi tecnologici rispettosi dei requisiti contemplati dai suddetti *standard*, si avrà l'opportunità di ridimensionare il rischio che gli stessi producano risultati inattendibili o in violazione delle normative in vigore.

[50] Sul punto v. LO SAPIO, *La trasparenza sul banco di prova dei modelli algoritmici*, cit., 243.

2. Nuove tecnologie, sistema penale e tutela dei diritti

Se appaiono innegabili i benefici che possono derivare dall'impiego delle tecniche di intelligenza artificiale in ogni branca della società[51], tanto da far propendere per un'intensificazione dello stesso[52], non sono da rinnegare il compendio di rischi che si celano dietro l'utilizzo delle nuove tecnologie a danno dei diritti umani.

Ben consapevole della questione risulta essere l'Alto Commissario delle Nazioni Unite per i Diritti Umani Volker Turk, il quale ha manifestato le sue preoccupazioni in merito all'utilizzo dei nuovi paradigmi di intelligenza artificiale poiché idonea a generare rilevanti violazioni in materia di diritti, arrecando danni, in modo particolare, alla dignità umana.

È per il suddetto motivo che lo stesso ha avanzato un appello urgente sia agli enti privati che ai diversi Stati sovrani affinché elaborino nel breve termine un compendio di misure volte a tutelare e a salvaguardare i diritti vantati da tutti gli esseri umani in quanto tali, dimostrandosi disponibile a collaborare e ad offrire un contributo basato sulla propria esperienza[53].

Edotto del rapporto conflittuale che sussiste tra intelligenza artificiale e diritti risulta essere altresì il Consiglio d'Europa, organismo che nei mesi precedenti alla pubblicazione della Carta Etica Europea[54], ha commissionato uno studio in merito all'impatto nocivo provocato dagli algoritmi sui diritti comuni a tutti gli esseri umani. Il mandato di ricerca è stato conferito al *Commitee of experts on internet intermediaries* (MSI-NET), un comitato scientifico composto da tredici esperti di diritto e nuove tecnologie al quale è stato affidato il compito di offrire una panoramica delle

[51] L'IA si dimostra utile ad offrire un notevole contributo per il raggiungimento di risultati di segno positivo a livello sociale e risulta in grado di migliorare le economie europee, rendendo più competitive le imprese del tessuto economico comunitario. In aggiunta, le nuove tecnologie contribuiscono al miglioramento nel fare previsioni, all'ottimizzazione delle operazioni e alla più efficiente assegnazione delle risorse e alla personalizzazione dell'erogazione di servizi, sul punto v. Proposta europea per la regolamentazione dei sistemi di IA, 20.

[52] L'obiettivo più ambizioso dichiarato nella proposta di regolamento europeo consiste nel rendere l'UE una leader nel settore delle nuove tecnologie.

[53] V. BALOCCO, *Intelligenza artificiale, allarme ONU: "Grave minaccia per i diritti umani*", in *CORCOM*, 2023. *https://www.corrierecomunicazioni.it/digital-economy/intelligenza-artificiale-allarme-onu-grave-minaccia-per-i-diritti-umani/*

[54] Si fa riferimento al biennio 2016-2017

possibili violazioni dei diritti umani ad opera degli algoritmi intelligenti[55], e si è concluso nel 2017 con la pubblicazione del *paper* intitolato *Algorithms and Human rights*.

Il testo in questione consta sì di una *pars destruens*, la quale contiene una sintesi delle principali zone d'ombra connesse all'impiego dei nuovi paradigmi tecnologici ed attesta una violazione di almeno otto diritti fondamentali da parte dei software di IA, ma non si limita a quest'ultima, tanto che le ultime pagine del *paper* contengono una *pars construens* volta ad illustrare nove suggerimenti rivolti agli Stati, utili a ridurre al minimo gli effetti negativi connessi all'impiego delle nuove tecnologie[56].

Il comitato di ricerca se, da un lato, si mostra consapevole che il numero di rischi di violazione dei diritti sia direttamente proporzionale al grado di complessità e di pervasività delle nuove tecnologie nelle vite di tutti i giorni[57], dall'altro afferma con convinzione che proibire l'utilizzo dell'intelligenza artificiale o arrestarne lo sviluppo non risulta essere una valida soluzione. Gli algoritmi vengono definiti infatti come «costrutti profondamente sociali» in quanto gli *output* prodotti dagli stessi non hanno alcun significato senza un sistema sociale di contorno che gliene attribuisca uno ben preciso[58]. È quindi troppo semplice incolpare il *software* per eventuali violazioni o suggerire di non ricorrere più alla tecnologia o all'informatica in generale. Piuttosto, sono il costrutto sociale, i valori incorporati negli algoritmi nonché i processi decisionali che interessano gli stessi che devono essere messi in discussione ed esaminati alla luce del loro impatto nocivo sui diritti umani.

Il primo diritto che lo studio "*Algorithms and human rights*" considera a rischio di violazione da parte dei nuovi *tools* è quello del giusto processo, il quale trova una puntuale formulazione nell'art 6 della CEDU.

Secondo il *Committe*, il crescente utilizzo dei paradigmi di intelligenza artificiale nel sistema di giustizia penale per prevenire la

[55] Sul punto v. Consiglio d'Europa, *Algorithms and Human rights*, 1. *https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5*
[56] In argomento v. Consiglio d'Europa, *Algorithms and Human rights*, cit., 4.
[57] Cfr. Consiglio d'Europa, *Algorithms and Human rights*, cit., 4 ss.
[58] V. Consiglio d'Europa, Algorithms and Human rights, 8.

commissione di un reato, identificare possibili soggetti attivi, calcolare un tasso di propensione al crimine sulla basa del passato di una persona fisica, nell'ambito di quella che prende il nome di polizia predittiva, sarebbe idonea a comportare una violazione del principio di presunzione di l'innocenza, del diritto di essere tempestivamente informati della causa e della natura di un'accusa, del diritto ad un processo equo e del diritto a difendersi di persona, tutte estrinsecazioni del *right to a fair trial*[59].

Alla luce di quanto rilevato dallo studio, le pratiche di polizia predittiva sarebbero altresì idonee a mettere a repentaglio sia l'articolo 5 della CEDU, che protegge contro la privazione arbitraria della libertà, che l'articolo 7 del medesimo testo normativo, avamposto del principio fondamentale del *nulla poaena sine lege*[60].

Il secondo diritto messo a repentaglio dall'impiego dei *software* è quello alla *privacy*[61]. Risulta ormai fuori discussione l'abilità degli algoritmi "intelligenti" di facilitare la raccolta, l'elaborazione e l'analisi di grandi quantità di dati eterogenei tra di loro. Questa circostanza, se da un lato viene a configurarsi come una potenzialità da sfruttare in molteplici ambiti, dall'altro può celare gravi violazioni del diritto ad avere una vita privata e familiare, così come del diritto alla protezione dei dati per come formulato dall'articolo 8 della CEDU.

L'utente che si avvale delle nuove tecnologie è costantemente sottoposto ad attività di profilazione[62], la quale consiste nell'impiego di processi di raccolta automatizzata per estrapolare l'insieme dei dati

[59] Sul punto v. Consiglio d'Europa, Algorithms and Human rights, cit., 10 ss.

[60] In generale, la Proposta di regolamento europea sull'intelligenza artificiale (AI ACT), si prepone l'obiettivo di assicurare le diverse declinazioni del diritto di difesa quali il diritto ad un ricorso effettivo, ad un giudice imparziale e la presunzione di innocenza previsti dalla Carta dei diritti fondamentali dell'Unione europea, sul punto v. Commissione europea, *Proposta di regolamento del parlamento europeo e del consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione*, Bruxelles, 2021, COM (2021) 206 final.

[61] In argomento v. Consiglio d'Europa, Algorithms and Human rights, cit., 12 ss.

[62] L'attività di profilazione viene definita dall'articolo 4 GDPR come «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»

personali disponibili su *Internet*, utili alla creazione di un profilo standardizzato dell'utente in questione. Lo studio dimostra come ogni persona fisica che si avvalga dei *software* sia soggetta ad un «rischio di sorveglianza su larga scala»[63] da parte sia di enti privati che di soggetti di diritto pubblico, i quali si avvalgono dei nuovi paradigmi tecnologici per individuare caratteristiche personali, preferenze e bisogni di un determinato individuo nell'ottica di sfruttare le stesse per finalità economiche, commerciali e politiche, ignorando l'indebita ingerenza che determinano nella sfera privata del cittadino[64].

Il conflittuale rapporto tra diritto alla *privacy* e impiego delle nuove tecnologie a supporto dell'attività di profilazione è stato in ultimo affrontato dal Regolamento UE 2026/679 (GDPR), volto a disciplinare lo sfruttamento dei dati personali a livello comunitario. Il suddetto testo normativo delinea dei veri e propri *standard* d'uso degli algoritmi e, agli articoli 13, 15 e 22, introduce il principio della trasparenza algoritmica, il quale si sostanzia nel diritto in capo all'utente alla conoscibilità, spiegabilità e nella comprensibilità del trattamento automatizzato[65].

È a danno del diritto di assemblea ed associazione disciplinato dall' articolo 11 della Convenzione europea dei diritti dell'uomo da rintracciare la terza potenziale violazione derivante dall'utilizzo delle nuove tecnologie[66]. Il progetto di ricerca commissionato dal Consiglio d'Europa dimostra come gli strumenti tecnologici, in modo particolare i *social media*, svolgano un ruolo di primo piano nell'organizzazione di occasione di pubblico confronto come manifestazioni, assemblee e proteste. La potenzialità offerta dai *tools* di tracciare e profilare un individuo *online* ed la contestuale possibilità per le pubbliche autorità di controllare la folla dei

[63] Sul punto v., Consiglio d'Europa, *Algorithms and Human rights*, 13.
[64] Lo stesso Consiglio dei diritti umani delle Nazioni Unite si è pronunciato in data 22 marzo 2017 per evidenziare gli effetti dannosi derivanti dalle attività di profilazione degli individui, osservando che il trattamento automatico dei dati personali per la profilazione individuale può comportare una discriminazione tra gli utenti e le decisioni assunte sulla base delle stesse influenzano negativamente il godimento di diritti umani, compresi i diritti economici, sociali e culturali, v. Consiglio d'Europa, *Algorithms and Human rights*, 13.
[65] Per un approfondimento sul punto si rimanda al paragrafo dedicato all'opacità degli algoritmi di intelligenza artificiale
[66] Sul punto v. Consiglio d'Europa, *Algorithms and Human rights*, cit., 22 ss.

manifestanti *off-line*, vengono considerato dal *Committee* come un forte deterrente a partecipare alle diverse manifestazioni di pubblica aggregazione, comportando pertanto violazione dell' articolo 11 ECHR in virtù del quale qualsiasi restrizione al diritto alla libertà di riunione pacifica e libertà di associazione deve essere prescritto dalla legge e deve perseguire uno scopo legittimo e necessario in una società democratica.

La quarta violazione prospettata dallo studio "*Algorithms and Human rights*" riguarda il diritto ad un rimedio effettivo. Quest'ultimo è contemplato dall'articolo 13 della Convenzione europea dei diritti dell'uomo, il quale garantisce ad ogni persona vittima di una violazione di un diritto umano la possibilità di avvalersi di un rimedio effettivo dinanzi a un'autorità nazionale. Il suddetto testo normativo prescrive pertanto agli Stati di garantire ai cittadini un accesso a procedimenti giudiziari o di altro tipo[67] affinché gli stessi decidano in modo imparziale in merito ad eventuali violazione dei diritti umani.

La CEDU precisa altresì che sussiste un onere anche in capo agli enti privati di garantire un effettivo rimedio alle vittime di una violazione dei diritti nella propria giurisdizione, a partire dalla previsione di meccanismi di reclamo volti a segnalare qualsiasi incongruenza nel breve termine.

I processi decisionali automatizzati, in virtù dell'opacità che li caratterizza, dell'impiego di dati personali e delle difficoltà a definire i diversi profili di responsabilità, mettono in seria discussione il diritto di ottenere un *effettive remedy* spettante alla generalità dei consociati, è per questo motivo che il *Committee* auspica che i soggetti sia pubblici che privati, nel momento in cui decidono di avvalersi dei *software* intelligenti a vario titolo, prospettino strumenti efficaci per evitare *ex ante* o sanare *ex post* eventuali violazioni dei diritti da parte delle tecnologie.

Un altro diritto umano considerato dal *paper* a rischio di violazione da parte dalle operazioni di trattamento automatizzato basate su algoritmi, è

[67] Vengono ricompresi efficaci meccanismi non giudiziari, ricorsi amministrativi e l'accesso alle istituzioni internazionali a tutela dei diritti umani

quello di godere dei diritti umani e delle libertà fondamentali senza discriminazione alcuna[68].

Se da un lato gli algoritmi potrebbero apparire come strumenti oggettivi ed imparziale pertanto utili a ridurre i pregiudizi e luoghi comuni nella conduzione di attività quali, ad esempio le operazioni di assunzione nel mondo del lavoro, in realtà il Comitato di esperti ha dimostrato come l'automazione e l'apprendimento automatico comportino l'effetto opposto, rafforzerebbero infatti i pregiudizi esistenti perché, a differenza degli esseri umani, non sono in grado di avere contezza e quindi contrastare consapevolmente i preconcetti irrazionali in cui si imbattono[69].

Il *Committee* incaricato dal Consiglio d'Europa sostiene che sussistono due diverse declinazioni di discriminazione, quella diretta e quella indiretta. Se gli algoritmi si dimostrano particolarmente abili ad escludere la prima, la quale si verifica quando una decisione si basa su criteri quali etnia, religione, genere, orientamento sessuale ed età alla luce di un pregiudizio inconscio nutrito dalla persona fisica, lo stesso non può dirsi in relazione alla seconda tipologia di discriminazione.

Quest'ultima si verifica quando una determinata cerchia di soggetti viene posta in una posizione di svantaggio alla luce di uno specifico fattore che li caratterizza o che si verifica con maggior frequenza[70]: agli stessi verrà infatti dedicato un trattamento differenziato in assenza di un valido motivo.

Dal momento in cui i *tools* operano analizzando dati e determinando correlazioni tra le informazioni processate, il rischio è che gli stessi siano portati a creare stereotipi idonei ad acuire le diverse possibili manifestazioni di discriminazione indiretta. Alla luce dei fatti, gli esperti consigliano di accertarsi che le decisioni assunte dai *software* non siano basate su differenziazioni ingiustificate e di programmare gli stessi in un modo tale da escludere una simile modalità di procedere.

---

[68] Diritto contemplato dall'articolo 14 ECHR

[69] Cfr. Consiglio d'europa, *Algorithms and human rights*, cit., 26 ss.

[70] Il Comitato fornisce un duplice esempio: la circostanza per cui un soggetto si una certa etnia viva in una certa area geografica o il dato alla luce del quale le donne che hanno avrebbero meno anni pensionabili a causa di interruzioni di carriera v. Consiglio d'Europa, *Algorithms and Human rights*, cit., 28.

Procedendo oltre nell'analisi di quanto prospettato dallo studio "*Algorithms and Human rights*", è da rinvenire nei diritti in capo ai lavoratori un'ulteriore area a rischio di violazione da parte dell'impiego dei nuovi paradigmi tecnologici. Negli ultimi anni si è andato progressivamente ad intensificare il ricorso agli algoritmi nell'assunzione di decisioni connesse al mondo del lavoro. I *tools* assurgono infatti a valido supporto nella conduzione di operazioni di *recruiting* del personale così come per l'assunzione di decisioni in materia di licenziamenti, questi ultimi contribuiscono inoltre all'organizzazione e alla gestione del personale e vengono impiegati per condurre le periodiche valutazioni dei lavoratori dipendenti.

Le preoccupazioni legate all'utilizzo dei nuovi paradigmi tecnologici in questo ambito sono connesse alla mancanza di trasparenza degli stessi, non sempre risulta infatti possibile comprendere l'*iter* tecnico e logico compiuto dalla macchina prima di fornire una determinata soluzione, con conseguente violazione del diritto alla *privacy* e del correlato principio della trasparenza algoritmica, entrambi disciplinati dal GDPR.

L'ultimo diritto menzionato dal paper in esame è il c.d. *right to free elections* contemplato dall'articolo 3 del protocollo n. 1 della Convenzione europea sui diritti dell'uomo[71].

I membri del *Commettee* evidenziano come l'intensa attività di profilazione al quale è sottoposto quotidianamente l'utente determina la creazione delle c.d. «*filter bubbles*», vale a dire contesti informativi dove vengono sottoposte all'utente soltanto le notizie o i contenuti che corrispondono al suo profilo, omettendo tutto ciò che viene considerato dall'algoritmo come estraneo o non rispondente alle preferenze o ai bisogni del soggetto. Questo *modus operandi* determina, da un lato, un rafforzamento delle opinioni e della linea di pensiero già sposata dalla persona fisica, dall'altro un allontanamento sempre maggiore da punti di vista diversi dal proprio. Quel che ne deriva è un impoverimento generale a

[71] L'art 3 del Protocollo 1 ECHR recita «Le Alte Parti contraenti si impegnano a organizzare, a intervalli ragionevoli, libere elezioni a scrutinio segreto, in condizioni tali da assicurare la libera espressione dell'opinione del popolo sulla scelta del corpo legislativo.»

livello culturale ed informativo in quanto viene negata all'utente la possibilità di confrontarsi con più linee di pensiero nonché una tendenza ad influenzare lo stesso in una direzione, negandogli la libertà di convincersi liberamente su un tema in particolare[72].

Tutto ciò, secondo gli esperti, può avere effetti cruciali sulla politica, specialmente nei periodi storici in cui si verificano le elezioni nei paesi democratici. Gli algoritmi di cui si avvalgono le nuove tecnologie, in modo particolare i *social media,* contribuiscono alla creazione di bolle ideologiche in grando di manipolare il pensiero politico del singolo e alterando l'opinione pubblica generale. È per questo motivo che i dati di cui si avvale l'intelligenza artificiale sono state definiti «la nuova moneta del potere»: la raccolta e l'analisi degli stessi contribuisce notevolmente alle operazioni di *microtargeting* degli elettori, con effetti determinati circa l'esito finale delle elezioni.

Quanto sopra prospettato risulta essere potenzialmente idoneo a mettere in pericolo l'integrità del processo elettorale, con conseguente violazione del diritto alle elezioni libere, riconosciuto dalla Corte europea dei diritti del l'uomo come «principio fondamentale in un regime politico veramente democratico»[73]

Secondo i membri del Comitato di esperti presso il Consiglio di Europa, il *vulnus* è da rinvenire nella mancanza di una regolamentazione adeguata in materia. Se infatti le emissioni televisive pubbliche sono generalmente tenute a garantire un certo livello di visibilità alle diverse componenti politiche nel rispetto del principio della *par condicio,* lo stesso non può dirsi per le piattaforme *social*, totalmente rimesse alla libertà dei privati. È in questa direzione, pertanto, che il *Commette* consiglia di intervenire, introducendo principi e disposizioni volti a regolamentare la materia così da limitare influenze indebite e monopoli della pubblica informazione.

[72] Sul punto v. Consiglio d'Europa, *Algorithms and human rights*, cit., 30 ss.
[73] In argomento v. EUROPEAN COURT OF HUMAN RIGHTS, *Guide on Article 3 of Protocol No. 1 to the European Conventionon Human Rights,* 1 ss. *https://www.echr.coe.int/Documents/Guide_Art_3_Protocol_1_ENG.pdf*

Una volta illustrata la *pars destruens* del lavoro di ricerca "*Algoritms and Human rights*", risulta utile passare in rassegna la componente propositiva, la quale si sostanzia in nove indicazioni principali elaborate dal Comitato di Esperti ed indirizzate, in modo particolare, agli Stati membri.

Le questioni relative alla *governance* algoritmica e alla regolamentazione delle nuove tecnologie vengono infatti considerati ambiti di pubblica competenza da non demandare interamente agli attori privati, fermo restando l'onere in capo a questi ultimi di adottare misure volte ad incrementare la trasparenza delle attività poste in essere e il dovere di garantire il rispetto dei diritti umani facenti capo ai propri utenti[74].

Il primo suggerimento è rivolto sia agli enti pubblici che agli attori indipendenti non statali. Gli esperti consigliano a questi ultimi di avviare ricerche e studi con l'obiettivo di comprendere meglio le implicazioni etiche e giuridiche in materia di diritti umani derivanti dal ricorso ad un procedimento decisionale algoritmico.

Quanto alla seconda indicazione, quest'ultima concerne i profili di responsabilità. Secondo il *Commette* gli enti pubblici dovrebbero essere ritenuti responsabili delle decisioni che adottano sulla base di processi algoritmici. Quest'ultimo auspica altresì l'introduzione di meccanismi che consentano alle vittime di una violazione e ai destinatari di una decisione automatizzata impropria di ottenere un risarcimento nel minor tempo possibile.

Il terzo suggerimento rinviene la propria *ratio* nella prevenzione di irregolarità e violazioni da parte delle tecnologie e si sostanzia nell'introduzione di operazioni di valutazione e di monitoraggio degli algoritmi in un momento preventivo al loro utilizzo ufficiale, così da evitare l'impiego di *tools* idonei ad arrecare violazioni di ogni genere.

Venendo al quarto consiglio, quest'ultimo si basa sull'importanza di coinvolgere e rendere consapevole la generalità dei consociati in merito ai diversi impieghi possibili dei *software* intelligenti. Viene infatti considerato doveroso per gli enti privati che si avvalgono dei nuovi paradigmi

[74] Cfr. Consiglio d'Europa, *Algorithms and human right*s, cit., 45 ss.

tecnologici per assumere decisioni di dare il via a campagne di informazione ed alfabetizzazione mediatica utili a garantire che tutti gli utenti comprendano a pieno le modalità di funzionamento delle tecnologie, la logica sottesa alle decisioni che assumono nonché i rischi in cui si imbatto avvalendosi degli stessi.

Il quinto ed il sesto consiglio forniti dagli esperti si ricollegano in qualche modo al terzo sopra esplicitato. Gli stessi consistono rispettivamente nella previsione di specifici meccanismi di certificazione e di revisione per gli algoritmi in modo da accertarsi a monte che questi ultimi siano rispettosi dei diritti umani e nell'obbligo di utilizzare tecniche automatizzate per monitorare le informazioni che trasmesse, archiviate o rese disponibili alla generalità degli utenti per contenere il rischio di incorrere in violazioni del diritto alla *privacy* dei soggetti interessati dalle stesse.

Il settimo monito è rivolto principalmente agli enti pubblici. Secondo il *Committee* questi ultimi dovrebbero adoperarsi affinché le proprie autorità di regolamentazione di settore sviluppino norme ed orientamenti specifici che garantiscano una risposta adeguata alle sfide che quotidianamente vengono alla luce in relazione all'impiego di decisioni automatizzate.

È nella necessità di prevedere nuovi enti, istituzioni, reti e spazi volti ad analizzare le diverse declinazioni di decisioni adottate dai *software* e le relative conseguenze derivanti dalle stesse da rinvenire l'ottava indicazione fornita dagli esperti in materia, uno sforzo che, secondo questi ultimi, andrebbe sostenuto da tutte le parti coinvolte.

Per concludere, il *Committee* è convinto che il Consiglio d'Europa sia la sede appropriata per esaminare ulteriormente gli impatti nocivi che l'impiego dei nuovi paradigmi tecnologici producono a danno dei diritti umani, in quanto quest'ultima rappresenta la principale organizzazione volta a tutelare gli stessi nel mondo. Il Consiglio d'Europa dovrebbe infatti impegnarsi affinché gli Stati membri sviluppino gli strumenti normativi idonei a regolamentare la materia[75].

[75] V. Consiglio d'Europa, *Algrithms and Human rights*, cit., 45 s.

I risultati dello studio "Algorithms and human rights" pocanzi illustrati servono a fare chiarezza nonché e costruire una consapevolezza generalmente diffusa in merito ai lati oscuri della tecnologia e ai rischi che si incorrono quando ci si avvale della stessa in ogni ambito. Questi ultimi dovrebbero ispirare dapprima i legislatori europei e nazionali che si accingono a regolamentare i nuovi paradigmi tecnologici, andrebbero tenuti in considerazione anche da chiunque utilizzi a vario titolo gli strumenti digitali ed infine dovrebbero assurgere a valido supporto per le possibili vittime di violazione di un diritto fondamentale ad opera di un algoritmo.

Tale discorso è valido altresì nel momento in cui gli enti decidono di avvalersi delle nuove tecnologie. Avere contezza delle possibili conseguenze negative e dei rischi di violazione dei diritti umani dovrebbe essere un presupposto fondamentale per la creazione di un apparato di *digital criminal compliance* affidabile e sicuro.

2.1 Verso una cultura della *cybersecurity*: il Libro Bianco e il *Framework* Nazionale per la *Cybersecurity* e la *Data Protection* elaborati dal CINI

Due anni dopo la pubblicazione della Carta Etica Europea da parte del Consiglio d'Europa, anche l'Unione Europea ha deciso di muovere dei passi per incrementare una cultura improntata alla *cybersecurity*.

La presidente della Commissione europea Ursula Von der Leyen, già in sede di candidatura alla carica, aveva dichiarato di voler presentare una normativa che garantisse un approccio unitario e coordinato a livello europeo circa le implicazioni umane ed etiche dell'intelligenza artificiale attraverso la pubblicazione del programma politico "Un'unione più ambiziosa"[76]. Impegno politico al quale la presidente ha tenuto fede con la pubblicazione nel febbraio 2020 del c.d. "Libro bianco sull'intelligenza artificiale, un approccio europeo all'eccellenza e alla fiducia" [77], un testo

[76] Il programma politico in questione è disponibile al seguente link *https://op.europa.eu/it/publication-detail/-/publication/43a17056-ebf1-11e9-9c4e-01aa75ed71a1*

[77] Sul punto v. Commissione europea, *Libro bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia*, COM(2020) 65 *final*.

che elabora una strategia comunitaria volta a conseguire un duplice obiettivo: potenziare lo sfruttamento delle nuove tecnologie mediante la creazione di un «ecosistema di eccellenza»[78] tale da rendere l'Unione Europea una *leader* nel settore delle nuove tecnologie e prevenire i rischi legati a determinati utilizzi dell'intelligenza artificiale tramite la predisposizione di un «ecosistema di fiducia»[79] a garanzia del rispetto delle norme dell'UE.

Per il conseguimento del primo obiettivo, il documento in esame elabora un piano strategico che consta di sei azioni principali da intraprendere. Il primo *step* predisposto dal Libro Bianco riguarda l'aggiornamento e la revisione del piano coordinato adottato dalla Commissione in collaborazione con gli Stati Membri nel dicembre 2018 ed orientato alla promozione ed allo sviluppo dell'intelligenza artificiale in Europa[80]. Incentivo reso possibile grazie alla smobilitazione di ingenti quantità di denaro nel contesto unionale[81] resa possibile grazie alla messa a disposizione da parte dell'UE di risorse provenienti dai programmi Europa digitale ed Orizzonte Europa nonché dagli ulteriori dai Fondi strutturali e di investimento europei.

La seconda azione contemplata dal Libro Bianco mira a concentrare gli sforzi della comunità tutta nelle attività di ricerca e negli studi propedeutici all'innovazione. La Commissione si impegna pertanto ad agevolare la creazione di centri di prova e di eccellenza volti a coordinare gli investimenti provenienti dai singoli stati membri, dai privati e dall'UE, anche avvalendosi di un nuovo istituto giuridico creato *ad hoc*. L'obiettivo

[78] Locuzione utilizzata nel Libro bianco che indica un ambiente proficuo che ricomprende ricerca, risorse e collaborazione tra pubblico e privato per incentivare l'utilizzo delle tecnologie di intelligenza artificiale anche da parte delle piccole e medie imprese.

[79] Espressione menzionata nel Libro bianco che si riferisce alla creazione di un quadro normativo completo e unitario a livello europeo volto a prevenire e regolamentare i rischi e le violazioni dei diritti fondamentali dell'uomo connessi all'utilizzo degli algoritmi di IA e a garantire il rispetto della normativa comunitaria così da spronare i cittadini ad avvalersi delle nuove tecnologie

[80] Quest'ultimo prende il nome di "L'intelligenza artificiale per l'Europa", COM(2018) 237 *final*. Tale piano propone circa 70 azioni comuni per una cooperazione più stretta ed efficiente tra gli Stati membri e la Commissione in settori chiave quali la ricerca, gli investimenti, l'adozione da parte del mercato, le competenze e i talenti, i dati e la cooperazione internazionale. Si prevede che il piano durerà fino al 2027, con monitoraggi e revisioni periodiche

[81] Si è parlato di oltre 20 miliardi di EUR di investimenti totali annui nell'IA nell'Unione europea.

è quello di superare il quadro frammentario dei centri di esperienza, incapace di competere con i principali colossi a livello mondiale, e proporre un approccio sinergico e unitario per migliorare l'eccellenza degli stessi, attrarre i migliori ricercatori e canalizzare in maniera efficace gli investimenti.

La terza strategia messa in campo dal documento in esame riguarda il potenziamento delle conoscenze e delle competenze in materia. La Commissione si dimostra intenzionata ad istituire una rete di collegamento tra le università, i centri di ricerca e gli istituti di istruzione superiore a livello europeo, così da creare un ambiente di ricerca variegato e all'avanguardia, orientato alla creazione di corsi di laurea magistrale nel campo dell'IA.

Quarta azione da realizzare per creare il c.d. «ecosistema di eccellenza», riguarda il maggiore coinvolgimento delle piccole e medie imprese nel processo di adozione delle nuove tecnologie di intelligenza artificiale nel tessuto economico europeo, operazione da realizzarsi i due *step* principali. In *primis* la Commissione si è impegnata a sostenere economicamente le PMI con l'avviamento di un progetto pilota che ha visto l'investimento di 100 milioni di euro nel primo trimestre del 2020, volto a fornire finanziamenti con capitale di rischio per sviluppi innovativi nel campo dell'IA; in secondo luogo, la stessa ha assicurato la presenza di almeno un polo di innovazione digitale specializzato per Stato Membro, utile a formare e supportare le piccole e medie imprese sia a livello teorico che pratico circa il funzionamento delle nuove tecnologie ed i loro possibili impieghi.

La quinto passaggio del piano strategico comunitario guarda all'istituzione di un partenariato pubblico-privato, vale a dire un rapporto di collaborazione tra la componente pubblica e i massimi dirigenti delle società private interessate al fine di garantire un coordinamento negli studi e nell'attività di ricerca in materia di Intelligenza artificiale, collaborare con altri partenariati pubblico-privati facenti capo al programma Orizzonte

Europa e lavorare insieme per la creazione di strutture di prova e poli dell'innovazione digitale precedentemente menzionati.

L'ultimo *step* preso in considerazione dal Libro Bianco mira a promuovere l'adozione delle tecnologie di intelligenza artificiale nel settore pubblico mediante l'istaurazione di dialoghi tra la Commissione ed i principali settori pubblici[82] con l'obiettivo di predisporre un piano d'azione concordato[83] che agevoli lo sviluppo, la sperimentazione e l'impiego concreto dell'IA.

Quanto al secondo obiettivo da raggiungere, la Commissione è consapevole delle perplessità maturate sia dai cittadini comunitari che dalle imprese. Se primi temono di incorrere in violazioni dei propri diritti e di non essere in grado di difenderli a causa delle asimmetrie informative del processo decisionale algoritmico, le seconde sono restie ad investire nel settore delle nuove tecnologie a causa dell'incertezza giuridica vigente, manca infatti un quadro normativo unitario volto a regolamentare la materia non solo a livello nazionale ma anche e soprattutto a livello comunitario.

Per ovviare a tale sentimento di sfiducia che rappresenta uno dei principali avversari al concreto sviluppo dell'intelligenza artificiale nelle economie degli stati membri, la Commissione ha provveduto ad elaborare un piano che affronta gli effetti socioeconomici connessi all'impiego dell'intelligenza artificiale[84] ed ha istituito un gruppo di esperti ad alto livello che nell'aprile 2019 ha pubblicato un documento a conclusione degli studi in materia, intitolato "orientamenti per un'IA affidabile"[85] . Nel testo in questione, sono stati individuati i sette requisiti principali che devono sussistere al fine di garantire la qualità e la sicurezza dei sistemi di intelligenza artificiale. Questi ultimi si estrinsecano nella presenza di un intervento di sorveglianza da parte dell'uomo, dei connotati di robustezza

[82] Il documento menziona nello specifico le amministrazioni pubbliche, gli ospedali, i servizi di pubblica utilità, i trasporti e le autorità di vigilanza finanziaria

[83] Il Libro Bianco fa riferimento al "Programma di adozione dell'IA", che sosterrà gli appalti pubblici di sistemi di IA e contribuirà a trasformare le procedure stesse degli appalti pubblici.

[84] Si fa riferimento al piano COM(2018) 237 final

[85] Per un approfondimento sul punto v. *https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top.*

tecnica e sicurezza nei *software* impiegati, di un approccio improntato alla riservatezza e *governance* dei dati, della trasparenza negli algoritmi utilizzati, di un approccio a garanzia della diversità, non discriminazione ed equità ed infine di un impianto orientato al benessere sociale e ambientale.

È in un contesto come quello tracciato dal Libro Bianco, propenso ad abbracciare lo sviluppo tecnologico per migliorare le economie ma allo stesso tempo cosciente dei rischi connessi all'utilizzo degli stessi che deve muoversi l'ente intenzionato di avvalersi dei nuovi paradigmi digitali per lo svolgimento delle attività tipiche di impresa, inclusa quella di predisporre l'insieme dei paradigmi organizzativi idonei a prevenire i reati in azienda.

Sono molteplici le opportunità che si prospettano le società alla luce di quanto stabilito nel suddetto testo quali, in modo particolare, la possibilità di ampliare le conoscenze in ambito tecnologico in virtù degli studi promossi e commissionati a livello unionale, lo sfruttamento dei fondi predisposti ad hoc dall'Unione europea per incentivare le PMI a digitalizzare le operazioni di impresa e l'avvalersi del supporto garantito dal polo di innovazione digitale presente nel proprio Stato Membro per ricevere indicazioni e per risolvere le eventuali problematiche tecniche che dovessero venire alla luce.

La stessa conformità ai sette principi delineati dal documento "Orientamento per un'IA affidabile" pocanzi enucleati, rappresenta una valida possibilità per gli enti di attestare i livelli di qualità e sicurezza in capo a ciascun sistema digitale, connotati indispensabili in quanto propedeutici sia alla produzione di *output* attendibili da parte della macchina che al rispetto dei diritti fondamentali in capo ai soggetti interessati dal processo automatizzato.

La scelta operata da una società di digitalizzare le attività tipiche di impresa, incluso il ricorso alla *digital criminal compliance*, impiegando i nuovi paradigmi tecnologici a supporto del modello organizzativo contemplato dal d.lgs. 231/2001, comporta inevitabilmente un aumento del rischio di incorrere in un attacco cibernetico o in una violazione dei sistemi digitali impiegati in azienda.

Anche nel nostro Paese è andata progressivamente maturando la consapevolezza dei rischi *cyber* e del contestuale bisogno di prevedere delle misure *ad hoc* per prevenirli e contenerli. La principale minaccia che si prospettata è rappresentata dai cosiddetti *data breach*[86], vale a dire l'insieme delle metodologie idonee a sottrarre fraudolentemnte ed appropriarsi indebitabilmente di dati ed informazioni dai *database* di proprietà delle imprese private ed enti pubblici[87].

È proprio per impedire la verificazione di fenomeni come questo che è stato ideato il c.d. *Framework Nazionale per la cybersecurity*, di cui è stata presentata una prima versione nel 2015, il quale rappresenta il frutto di una proficua collaborazione tra università, enti pubblici ed imprese private.

Quest'ultimo, ispirandosi direttamente al *Framework* elaborato dal *National Institute of Standards and Tecnology* (NIST), delinea un modello da seguire per organizzare l'insieme dei processi di *cybersecurity* e si configura quale valido supporto sia per le organizzazioni pubbliche che private. L'attale formulazione del suddetto strumento si discosta parzialmente dalla prima formulazione, lo stesso è stato infatti sottoposto a recenti modifiche volte a recepire le indicazioni principali in materia di protezione dei dati introdotte in ultimo dal GDPR.

Il *Framework* attualmente in vigore consta di tre elementi costitutivi principali. Il primo prende il nome di *Framework Core*[88], il quale costituisce la vera e propria struttura del modello idoneo ad implementare la cultura della *cybersecurity*. Quest'ultimo è suddiviso a sua volta in *function, category e subcategory*, dove le *function* rappresentano gli obiettivi da perseguire per una corretta gestione del rischio e si sostanziano

[86] Definito dal Garante Privacy come "una violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati", sul punto v. *https://www.garanteprivacy.it/data-breach*

[87] V. Framework Nazionale per la cybersecurity, 2019, 8 s. *https://www.cybersecurityframework.it/framework2*

nell'*identify*[89]*, protect*[90]*, detect*[91]*, respond*[92]*, recover*[93]. Il *Framework* a sua volta riconduce ad ogni *function* un compendio di *category* e *subcategory*, vale a dire l'insieme delle azioni e procedure da adottare per conseguire la finalità alle quali sono associate. .

Il secondo elemento costitutivo è rappresentato dai c.d. profili, i quali si estrinsecano nell'esito dell'attività di selezione delle diverse *subcategory* alla luce di fattori quali l'attività economica poste in essere dall'ente, l'entità dei rischi in cui è possibile incorrere e la fattibilità in concreto delle diverse *subcategory*. Gli stessi vengono impiegati per definire le priorità, attestare i progressi e conseguire dei miglioramenti[94] così come per effettuare un'autovalutazione del modello predisposto dall'ente

Il terzo ed ultimo elemento costitutivo del *Framework* è rappresentato dall' *Implementation Tier* , vale a dire dei livelli di valutazioni che consentono all'ente pubblico o privato di avere contezza dell'efficacia del modello predisposto nel prevenire e gestire i rischi *cybe*r. Attualmente

---

[89] L'obiettivo di *identify* consiste «nella comprensione del contesto aziendale, degli asset che supportano i processi critici di business e dei relativi rischi associati la quale permette a un'organizzazione di definire risorse e investimenti in linea con la strategia di gestione del rischio e con gli obiettivi aziendali». Le category all'interno di questa function sono: *Asset Management, Business Environment; Governance, Risk Assessment,Risk Management Strategy, Supply Chain, Risk Management e Data Management*", sul punto v. Framework Nazionale per la cybersecurity, 2019, cit., 9 s.

[90] Per *protect* si intende «l'implementazione di quelle misure volte alla protezione dei processi di business e degli asset aziendali, indipendentemente dalla loro natura informatica». Le *category* all'interno di questa *function* sono: *Identity Management, Authentication and Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, Protective Technology*", sul punto v. Framework Nazionale per la cybersecurity, 2019, cit., 9 s.

[91] La funzione di *detect* è associata «alla definizione e attuazione di attività appropriate per identificare tempestivamente incidenti di sicurezza informatica». Le category all'interno di questa function sono: *Anomalies and Events, Security Continuous Monitoring, Detection Processes*" cfr. Framework Nazionale per la cybersecurity, 2019, cit., 9 s

[92] Per *respond* si intende «la definizione e attuazione delle opportune attività per intervenire quando un incidente di sicurezza informatica sia stato rilevato. L'obiettivo è contenere l'impatto determinato da un potenziale incidente di sicurezza informatica». Le *category* all'interno di questa *function* sono: *Response Planning, Communications, Analysis, Mitigation, Improvements*" v. Framework Nazionale per la cybersecurity, 2019, cit., 9 s

[93] Quanto alla *recover*, quest'ultima implica la «definizione e attuazione delle attività per la gestione dei piani e delle attività per il ripristino dei processi e dei servizi impattati da un incidente. L'obiettivo è garantire la resilienza dei sistemi e delle infrastrutture e, in caso di incidente, supportare il recupero tempestivo delle *business operations*». Le *category* all'interno di questa *function* sono: *Recovery Planning, Improvements, Communications" v.* Framework Nazionale per la cybersecurity, 2019, cit., 9 s

[94] La pratica più comune consiste nel confronto tra il profilo attualmente adottato, che prende il nome di profilo corrente, e quello che si ha l'obiettivo di porre in essere, vale a dire il profilo *target*

sono previsti quattro diversi livelli di valutazione, quello parziale, quello informato, quello ripetibile e quello adattivo[95].

Il primo menzionato è da considerarsi il livello più debole, quest'ultimo si configura quando l'ente in questione non ha tenuto conto in maniera completa di tutti i possibili rischi connessi all'attività esercitata in concreto e l'approccio che adotta tende ad essere reattivo più che preventivo. Il secondo livello presenta profili di maggiore sviluppo rispetto al primo, esso si verifica quando l'organizzazione presenta dei processi interni che tengono conto del rischio *cyber*, ma che ancora presentano scarsi livelli di pervasività in quanto non si estendono a tutta l'organizzazione.

Il livello c.d. ripetibile viene conseguito quando il modello adottato è soggetto ad un aggiornamento costante alla luce dei risultati derivanti dalle operazioni di risk management. In questo caso la gestione del rischio *cyber* è pervasiva a tutti i livelli organizzativi ed il personale è formato per gestire i ruoli che in merito gli vengono assegnati. In aggiunta, organizzazione è confrontarsi con gli atti soggetti che operano nel medesimo contesto circa gli espedienti adottati in ambito *cybersecurity*.

L'ultimo livello contemplato è quello c.d. adattivo, quest'ultimo risulta essere il più all'avanguardia dei quattro e si verifica qualora l'ente dimostri di adottare un compendio di procedure orientate alla prevenzione del rischio, elaborate alla luce delle esperienze passato e degli indicatori sviluppati. In aggiunta, l'organizzazione complessa deve dare conto dell'opera di adeguamento costante del modello, in modo da rendere lo stesso capace di rispondere efficacemente ad ogni tipo di attacco.

Alla luce di quanto delineato, si ritiene che il *Framework* per la *Cybercycurity* pocanzi analizzato costituisca un valido supporto per gli enti in quanto si sostanzia in un compendio di linee guida utile alle imprese che intendono avvalersi dei nuovi strumenti tecnologici in azienda e vogliono garantire la sicurezza e l'inaccessibilità di questi ultimi per abbattere il rischio di incorrere in un *data breach*.

[95] In argomento v. Framework nazionale per la *cybersecurity*, cit., 10 s.

3. Il criterio di imputazione oggettiva in presenza di un a*lgorithmic misconduct*

Una questione cruciale da affrontare nell'estrinsecazione dei rischi e delle zone d'ombra connessi alla *digital criminal compliance,* riguarda i profili di responsabilità per l'ente in presenza di un «*algorithm misconduct*»[96], vale a dire nel momento in sia stato il *tool* "intelligente" a porre in essere un'operazione idonea a consentire/favorire l'integrazione di una delle fattispecie criminose contemplate nel d.lgs 231/2001.

Innanzitutto, appare opportuno chiarire quali siano gli elementi che devono sussistere al fine di ritenere una persona giuridica responsabile di un reato commesso al suo interno. Il legislatore del 2001, con l'obiettivo di disattendere il brocardo *societas delinquere non potest*, ha deciso di individuare in due variabili principali gli elementi costituitivi del *tertrium genus* di responsabilità ascrivibile all'ente.

Il primo criterio è quello di imputazione oggettiva e trova una disciplina puntuale nell'articolo 5 del decreto 231/2001. Quest'ultimo consta di due componenti principali che si estrinsecano nella particolare qualifica che deve rivestire il soggetto attivo dell'illecito, condizione volta a testimoniare il rapporto funzionale/strutturale tra la persona fisica e la persona giuridica, e nella presenza dell'interesse o del vantaggio dell'ente[97], utili ad evidenziare un legame utilitaristico tra la fattispecie criminosa e l'ente[98].

Al fine di poter ritenere l'ente responsabile del reato verificatosi al suo interno, occorre pertanto che la fattispecie criminosa riconducibile ad uno dei reati tassativamente annoverati nel decreto sia stata commessa da un soggetto apicale o da un soggetto sottoposto, nell'interesse o a vantaggio dell'ente[99], con la precisazione ulteriore che l'ente sarà esente da

[96] Espressione utilizzata in DIAMANTIS, *The Problem of Algorithmic Corporate Misconduct*, in SSRN, 2019, 3.
[97] Profilo, quest'ultimo, non poco controverso e che ha dato adito ad un acceso dibattito in dottrina meritevole di una trattazione specifica nelle pagine che seguono.
[98] Cfr. BARTOLI, *Il criterio di imputazione oggettiva*, in LATTANZI, SEVERINO (*a cura di), La responsabilità da reato degli enti*, vol. I, Torino, 2021, 171 s.
[99] Ai sensi di quanto stabilito dal comma 1 dell'art 5 del d.lgs 231/2001.

responsabilità qualora uno dei soggetti sopra menzionati abbia agito nell'interesse esclusivo proprio o di terzi[100].

Questo primo livello di ascrizione del reato alla persona giuridica rappresenta l'espediente adottato dal legislatore per ricondurre una fattispecie criminosa all'ente, con l'obiettino di ottemperare ad uno dei principi cardine del diritto penale quale quello della responsabilità penale personale[101]. La soluzione adottata nel decreto fa leva sulla teoria dell'immedesimazione organica, in virtù della quale l'illecito posto in essere da un soggetto inserito nella compagine dell'ente e che, nell'esercizio delle funzioni tipiche, agisce nell'ottica di perseguire un interesse o un vantaggio per quest'ultimo, è reato dell'ente[102]. La stessa giurisprudenza concorda con il fatto che la compresenza di questa duplice condizione è idonea a configurare una responsabilità per fatto proprio in capo alla persona giuridica[103].

Le persone fisiche contemplate dal decreto sono i c.d. apicali ed i c.d. sottoposti e se tra gli stessi non sussiste alcuna differenziazione in relazione a questo primo criterio di responsabilità, il discorso si fa parzialmente diverso quanto al secondo livello di ascrizione del reato[104]. Per soggetto apicale si intende chiunque rivesta funzioni di rappresentanza, amministrazione e direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale. Al suddetto novero vanno aggiunti anche coloro che esercitano, anche di fatto, la gestione e il controllo della persona giuridica in questione poiché il criterio oggettivo funzionale contemplato all'articolo 5 del decreto 231 non si basa sulla qualifica formale

[100] Alla luce di quanto previsto dal comma 2 dell'art 5 del d.lgs 231/2001
[101] Principio contemplato nel primo comma dell'articolo 27 della Costituzione Italiana che recita testualmente "La responsabilità penale è personale".
[102] Sul punto v. BARTOLI, *Il criterio di imputazione oggettiva*, in LATTANZI, SEVERINO (*a cura di), La responsabilità da reato*, cit. 174 s.
[103] V. Cass., Sez. Un., 18 settembre 2014, n. 38343, in *DeJure*
[104] Si fa riferimento al criterio di imputazione soggettiva meritevole di un approfondimento specifico nel paragrafo successivo del medesimo capitolo

rivestita dal soggetto ma sulla funziona svolta in concreto da quest'ultimo[105].

Nello specifico, alla luce delle funzioni annoverate nell'articolo in esame, i soggetti apicali coincidono con i vertici dell'ente, vale a dire con gli amministratori e con i direttori generali di quest'ultimo. Ai primi spetta per natura la prima funzione menzionata, quella di amministrazione, la quale si sostanzia in quattro poteri principali quali quello di iniziativa, quello esecutivo, quello decisionale e quello rappresentativo. La seconda funzione è quella di rappresentanza e fa riferimento a quella organica, esercitabile da un amministratore nell'esercizio delle funzioni tipiche, da distinguere con quella volontaria propria di un soggetto sottoposto[106]. In ultimo, la funzione di direzione, la quale spetta ai direttori generali della persona giuridica, per questo motivo da includere nella definizione di soggetto apicale.

Da una lettura della norma non si evince alcun riferimento nei confronti dei sindaci. Viene infatti utilizzata la locuzione «gestione e controllo»[107] che fa sottintendere l'esclusione dei membri del CDA dal novero dei soggetti apicali. Questa soluzione, seppur parzialmente contestata da una parte della dottrina[108], trova conferma sia in quanto stabilito nella Relazione ministeriale che accompagna il decreto legislativo 231 del 2001, in virtù della quale il mero potere di controllo non rileverebbe se non accompagnato da quello di gestione, e dunque dall'esercizio di un vero e proprio «dominio»[109] sull'ente, che alla luce della Riforma societaria entrata in vigore nel 2003 la quale, nell'estendere la responsabilità dell'ente

[105] Per fornire un esempio in concreto, verrà considerato soggetto apicale anche il c.d. amministratore dipendente poiché, seppur in un rapporto di lavoro dipendente con l'ente, di fatto esercita le funzioni proprie di un amministratore.
[106] Sul punto v. DI GIOVINE, *Lineamenti sostanziali del nuovo illecito punitivo*, in LATTANZI (*a cura di*), *Reati e responsabilità degli enti. Guida al d.lgs. 8 giugno 2001, n. 231*, Torino, 2010, 58.
[107] Ai sensi del comma 2 dell'articolo 5 d.lgs 231/2001
[108] Lo stesso Bartoli fa una distinzione tra i reati propri dei sindaci e reati commessi dagli amministratori, in riferimento ai quali i membri del CDA potrebbero rispondere in concorso per omesso impedimento del reato, sostenendo che, almeno per la prima categoria di fattispecie criminose, i sindaci andrebbero ricompresi nel novero dei soggetti apicali, sul punto v. BARTOLI, *Il criterio di imputazione oggettiva*, in LATTANZI, SEVERINO (*a cura di), La responsabilità da reato,* cit., 181.
[109] Cfr. Relazione ministeriale al d.lgs n. 231/2001

anche ai reati societari, non ha effettuato alcun richiamato ai sindaci nell'art. 25-ter.

Oltre agli apicali, il criterio di imputazione oggettiva ricomprende un'ulteriore categoria di soggetti, i c.d. sottoposti. Questa denominazione fa riferimento alle persone fisiche soggette «alla direzione o alla vigilanza» degli apicali, vale a dire i lavoratori subordinati e parasubordinati. In questo caso si fa leva si sulla *vicarious liability*[110], in virtù della quale si rinviene una responsabilità in capo all'ente per i fatti posti in essere dai soggetti che compongono l'azienda[111], ma quest'ultima, nell'ordinamento italiano, non è considerata sufficiente da sola richiedendosi altresì l'elemento della direzione e della vigilanza a cura dei vertici dell'azienda.

La seconda componente propria di questo primo livello di ascrizione della responsabilità in capo alla persona giuridica è rappresentata dall'interesse o dal vantaggio che l'ente deve ricavare dalla commissione del reato da parte dei vertici della società o dei dipendenti della stessa. Il significato da dare ai concetti di interesse e vantaggio è stato oggetto di un acceso dibattito dottrinale che, per fini didascalici, è possibile semplificare nei termini che seguono. Negli anni immediatamente successivi all'entrata in vigore del decreto 231, parte della dottrina[112] si è resa fautrice della c.d. tesi monistica in virtù della quale l'interesse e il vantaggio sarebbero due concetti assimilabili tra di loro poiché connotati dalla medesima natura.

Questa linea di pensiero, sostenuta altresì da diverse pronunce giurisprudenziali[113], considera l'interesse come l'unico parametro concretamente rilevante ai fini dell'attribuzione della responsabilità, declassando l'elemento del vantaggio a mera variabile causale che, a

[110] Responsabilità basata sul principio del *respondeat superior*
[111] Sul punto v. SABIA, *Artificial intelligence and environmental criminal Compliance*, in ESPINOZA DE LOS MONTEROS DE LA PARRA, GULLO, MAZZACUVA (a cura di), *The Criminal Law Protectio*n, cit., 188.
[112] V. PULITANÒ, *La responsabilità "da reato" degli enti: i criteri di imputazione*, in *Riv. It. dir.proc. pen.*, 2002, 405; DE SIMONE, *La responsabilità da reato degli enti nel sistema sanzionatorio italiano: alcuni aspetti problematici*, in *Riv. Trim. dir. Pen. econ*., 2004, 671; SELVAGGI, *L'interesse dell'ente collettivo quale criterio di ascrizione della responsabilità da reato*, Napoli, 2006, 28 ss;
[113] Si fa riferimento alla Cass., 23 giugno 2006, n. 32627, in *Guida dir*., 2006, 42, 61 ss.

prescindere dal suo verificarsi, non è idonea ad ergersi a criterio di imputazione[114].

I sostenitori di questa prima teoria basano il proprio convincimento su tre argomentazioni principali. La prima fa leva sul testo dell'articolo 5 del decreto 231 del 2001 che, al secondo comma, contempla l'esclusione della responsabilità dell'ente in presenza dell'interesse esclusivo proprio dei soggetti apicali, sottoposti o di terze parti, omettendo di menzionare il parametro del vantaggio e facendo dedurre, da un'interpretazione letterale dello stesso, che si verifichi una rottura dell'immedesimazione organica a prescindere dalla presenza o meno di quest'ultimo[115].

Un secondo argomento in favore della tesi monistica guarda agli articoli 12, comma 1, lettera a) e 13, comma 3 del decreto, i quali prevedono una riduzione della pena per l'ente nel primo caso, e l'esclusione delle sanzioni interdittive nel secondo, qualora il soggetto arrivo del reato abbia agito «nel prevalente interesse proprio o di terzi» e la persona giuridica o non ne abbia ricavato un vantaggio per sé, o qualora l'avesse fatto, quest'ultimo sia stato di minima entità. Secondo i sostenitori di questa prima teoria, entrambe le disposizioni normative attribuirebbero un peso preponderante al parametro dell'interesse il quale potrà sussistere in maniera soltanto parziale e marginale, attuando una distinzione con il criterio del vantaggio che, al contrario, potrà anche concretamente mancare senza che tale circostanza conduca ad escludere la riduzione della pena da applicare.

In ultimo, i fautori della tesi volta ad assimilare interesse e vantaggio, sono dell'idea che attribuendo diversa natura ai due parametri, si andrebbe a verificare un contrasto con il primo comma dell'articolo 27 della Costituzione italiana: il dato del vantaggio, pertanto, è da considerarsi accidentale ed indipendente rispetto all'atteggiamento soggettivamente rimproverabile all'ente a titolo di colpa di organizzazione.

Alternativa alla tesi monistica è quella c.d. dualistica, teoria che prende in un momento successivo alla prima e che considera i criteri

[114] V. BARTOLI, *Il criterio di imputazione oggettiva*, in LATTANZI, SEVERINO (*a cura di), La responsabilità da reato*, cit., 186 s.
[115] Sul punto v. DE VERO, *La responsabilità penale delle persone giuridiche*, Torino, 2008, 158 s.

dell'interesse e del vantaggio come distinti ed alternativi tra di loro. Le argomentazioni addotte dalla dottrina sono principalmente due. La prima si basa sulla Relazione di accompagnamento al decreto 231 del 2001 la quale concepisce i due parametri in esame come indipendenti tra di loro[116], la seconda coincide con la terza argomentazione[117] sposata dai sostenitori della tesi monistica della quale, tuttavia, viene data una lettura diametralmente opposta. In questo caso, infatti, la menzione di entrambi i parametri da parte degli articoli 12 e 13 del decreto, viene interpretata come una valorizzazione della alternatività ed autonomia dei suddetti criteri[118].

La seguente teoria dualistica viene altresì accolta dalla giurisprudenza, la quale valorizza il parametro dell'interesse in un momento antecedente alla verificazione della fattispecie criminosa in quanto connota soggettivamente la condotta della persona fisica, mentre dà rilievo al criterio del vantaggio in una fase successiva all'esito del reato, poiché considera lo stesso come il beneficio oggettivo ricavato dall'ente che può verificarsi a prescindere da una sua intenzionale previsione *ex ante* da parte del soggetto attivo[119].

Un ulteriore contributo chiarificatore in materia viene offerto dalla legge n. 69 del 2015, rubricata "Disposizioni in materia di delitti contro la pubblica amministrazione, di associazioni di tipo mafioso e di falso in bilancio" la ha quale, modificando l'art. 25-ter d. lgs. n. 231/2001 in modo da eliminare il riferimento al solo criterio dell'interesse della società, ha reso

---

[116] «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 tale via la manifesta estraneità della persona morale, il giudice non dovrà neanche verificare se la persona morale abbia per caso tratto un vantaggio», come si evince dalla Relazione che accompagna il decreto 231 del 2001. Quest'ultima sembrerebbe confermare la tesi dualistica in quanto qualora la persona fisica avesse agito nel suo solo interesse, non potrebbe aver operato nell'interesse dell'ente e dunque non rileverebbe nemmeno la circostanza per cui l'ente abbia da ciò ricavato comunque un vantaggio *ex post*.

[117] Si fa riferimento agli articoli 12, comma 1, lettera a) e 13, comma 3, del d.lgs. 231/2001, rubricati rispettivamente come "Casi di riduzione della sanzione pecuniaria" e "Sanzioni interdittive".

[118] Cfr. DE VERO, *La responsabilità penale delle persone giuridiche*, Torino, 2008, 158.

[119] Di quest'idea Cass. pen., sez. II, n. 3615/2005, Jolly Mediterraneo s.r.l. in virtù della quale «I due vocaboli esprimono concetti giuridicamente diversi, potendosi distinguere un interesse "a monte" della società ad una locupletazione prefigurata, pur se di fatto, eventualmente, non più realizzata in conseguenza dell'illecito, rispetto ad un vantaggio obbiettivamente conseguito all'esito del reato, perfino se non espressamente divisato ex ante dall'agente»

irrilevanti le questioni interpretative sorte sulla formulazione previgente e ha concluso che dovrà farsi riferimento al criterio generale disciplinato dall'art. 5 del decreto, il quale attribuisce rilevanza al reato commesso «nell'interesse o a vantaggio» dell'ente.

Una volta illustrato il criterio di imputazione oggettiva, la cui verificazione risulta indispensabile per attribuire una responsabilità in capo alla persona giuridica, occorre fornire una risposta al quesito d'esordio del presente paragrafo. È opportuno, infatti, chiarire se il primo livello di ascrizione della responsabilità all'ente risulta integrato qualora il reato presupposto si sia verificato per via dell'incorretto funzionamento di un algoritmo di intelligenza artificiale, vale a dire in presenza di un *algorithm misconduct*.

Sul punto si rende necessario effettuare una distinzione tra quei paradigmi di IA che risultano ancora fortemente dipendenti dalla persona fisica che li ha programmati in quanto gli *input* di cui si avvalgono vengono forniti da quest'ultimo e gli *output* generati appaiono in gran parte prevedibili nonché comprensibili da parte del programmatore[120], e quei *software* "intelligenti" che, a differenza dei primi, presentano ampi profili di autonomia[121] poiché capaci di auto-apprendere dal *web* e dalle esperienze passate nonché soliti generare dei risultati attraverso passaggi tecnici che appaiono oscuri ed incomprensibili anche all'esperto di tecnologie che li ha predisposti[122].

Un primo profilo di differenza tra le due macrocategorie di IA consiste nell'attribuzione dei diversi profili di responsabilità, attività più agevole nel caso in cui la fattispecie criminosa si sia verificata con il contributo della prima tipologia di *tools*. Le tecnologie in questione, infatti,

[120] In relazione a questa prima tipologia di *software*, il "controllo umano" è ancora di notevole entità, sul punto v. PIERGALLINI, *Intelligenza artificiale:da 'mezzo' ad 'autore' del reato*?, Torino, 2020, 88.

[121] Si fa riferimento a quei sistemi di apprendimento automatico che si basano su tecniche di *machine learning* o, addirittura, *deep learning*.

[122] V. MOSCO, *Roboboard. L'intelligenza artificiale nei consigli di Amministrazione*, in *Analisi giuridica dell'economia*, 2019, 250; PIERGALLINI, *Intelligenza artificiale:da 'mezzo' ad 'autore' del reato*? cit., 89; SALVADORI, *Agenti artificiali, opacità, tecnologica e distribuzione della responsabilità penale*, cit., 60 ss; TRIPODI, Uomo, societas, machina, in *legislazione penale*, 2023, 10 ss.

non vengono a configurarsi come entità autonome ed indipendenti rispetto al programmatore in quanto quest'ultimo detiene ampi margini di libertà nel formattarle, è in grado di comprenderne i passaggi tecnici e ha la possibilità di prevedere e prevenirne i risultati prodotti.

Questi ultimi consistono pertanto in meri strumenti[123] di cui la persona fisica si avvale per il compimento di un'attività, la quale può ben consistere in una fattispecie criminosa. È per questo motivo che nel caso di specie appare possibile che a rispondere dei reati verificatesi a causa del malfunzionamento dei *software* sia la persona fisica, responsabile a titolo di colpa per non aver previsto ed evitato le incongruenze generate dalla macchina ovvero a titolo di dolo qualora abbia progettato la stessa con l'obiettivo di delinquere[124].

Alla luce delle suddette considerazioni, sembrerebbe configurarsi da un lato, un profilo di responsabilità in capo al programmatore/utilizzatore persona fisica, dall'altro, l'integrazione del criterio di imputazione oggettiva contemplato dall'articolo 5 del decreto 231 nel caso in cui il soggetto in questione appartenga all'organico dell'ente in qualità di apicale o sottoposto, verificandosi pertanto un'ipotesi di immedesimazione organica con l'ente.

In aggiunta, andrebbe accertato se sussiste una posizione di garanzia[125] in capo agli amministratori di una società nei confronti dell'operato delle macchine automatizzate[126], verificando in concreto la presenza dei tre profili indefettibili che la compongono, quali il corredo di poteri-doveri imposti dal diritto civile[127], l'accertamento dell'efficacia impeditiva dell'azione omessa nonché la sussistenza del dolo, anche eventuale.

---

[123] PIERGALLINI, *Intelligenza artificiale:da 'mezzo' ad 'autore' del reato?* cit., 88; V. BARTOLI, *Il criterio di imputazione oggettiva*, in LATTANZI, SEVERINO (*a cura di), La responsabilità da reato,* cit., 264.

[124] Cfr. SEVERINO, *Intelligenza artificiale e diritto penale*, in RUFFOLO (a cura di), *Intelligenza artificiale*, cit., 533 s.

[125] La posizione di garanzia è contemplata dall'articolo 40 del codice penale, in virtù del quale «non impedire un evento che si ha l'obbligo giuridico di impedire equivale a cagionarlo».

[126] In argomento v. NISCO, *Riflessi della compliance digitale in ambito 231*, cit., 9.

[127] Corredo di poteri e doveri che costituiscono l'obbligo giuridico che fonda e circoscrive la posizione di garanzia

Parte della dottrina[128] considera opportuno applicare le regole della *corporate governance* anche all'impiego degli algoritmi di intelligenza artificiale in ambito societario. Sussiste in capo agli amministratori il dovere di corretta amministrazione, dovere che si estrinseca principalmente nella garanzia circa l'adeguatezza degli assetti organizzativi, amministrativi e contabili della società[129]. Qualora si decida di avvalersi delle nuove tecnologie nella creazione di un modello organizzativo interno all'ente, appare opportuno porre in essere anche nei confronti delle stesse le attività di «cura», «valutazione» e «vigilanza» contemplate direttamente dagli articoli 2381 e 2403 del codice civile, le quali sono di competenza, rispettivamente, degli amministratori delegati, del consiglio di amministrazione e dell'organo di controllo.

In relazione al nesso causale, vale a dire all'efficacia impeditiva dell'azione che l'amministratore aveva il dovere di realizzare, va accertato se sussistono poteri preesistenti al comportamento dell'agente tecnologico che, se attivati, possono impedire la realizzazione del reato da parte dello stesso. Questi ultimi[130] non devono necessariamente consistere in poteri individuali direttamente impeditivi ma possono estrinsecarsi nella richiesta di intervento da parte di un soggetto terzo[131] capace di impedire il malfunzionamento del *tool* idoneo ad integrare una fattispecie criminosa.

Infine, quanto alla sussistenza dell'elemento soggettivo in capo all'amministratore, risulta opportuno dimostrare la consapevolezza dell'amministratore di avallare, attraverso la propria inerzia, l'attività criminosa resa possibile dal *software* di IA. Viene a configurarsi un dolo diretto nel caso in cui l'amministratore sia stato previamente informato della

[128] Sul punto v. MOSCO, *Roboboard. L'intelligenza artificiale nei consigli di Amministrazione*, cit., 254 s.

[129] Ai sensi dell'articolo 2086, comma 2, del codice civile, rubricato «Gestione dell'impresa» inserito ad opera dell'art.375 C.C.I. ed entrato in vigore il 16 marzo 2019

[130] In generale, l'amministratore non può direttamente impedire il compimento di reati perché non dispone di poteri individuali direttamente impeditivi. Egli può innescare il meccanismo in astratto idoneo a impedire la realizzazione di reati ma l'effettivo impedimento dell'evento presuppone sempre l'intervento di un soggetto terzo quali il pubblico ministero, il presidente del CdA, il consiglio di amministrazione stesso, il presidente del collegio sindacale, il giudice, l'autorità di vigilanza. Sul punto v. ALESSANDRI, SEMINARA, *Diritto penale commerciale*, vol I, Principi generali, Torino, 2018, 59.

[131] Come il programmatore stesso dell'algoritmo o un esperto di tecnologie

realizzazione di condotte illecite da parte della macchina automatizzata e abbia volontariamente omesso di intervenire; tuttavia, si ritiene sufficiente la presenza almeno del dolo nella forma eventuale alla luce delle asimmetrie informative che connotano il consiglio di amministrazione, elemento soggettivo che richiede comunque sia l'accertamento del momento rappresentativo, facendo ricorso alla c.d. teoria dei segnali di allarme, che la verificazione del momento volitivo, il quale coincide con l'accettazione dell'evento.

Al sussistere dei tre elementi sopra esplicitati, è possibile concludere circa la sussistenza di una posizione di garanzia in capo agli amministratori in relazione al funzionamento delle tecnologie di intelligenza artificiale adoperate nell'assetto organizzativo dell'ente, con la conseguenza che nel caso in cui il vertice dell'ente ometta di porre in essere le azioni impeditive doverose, verrà a configurarsi, ove sia possibile ravvisarne tutti i relativi presupposti, una responsabilità a carattere omissivo in capo allo stesso, la quale sarà a sua volta idonea ad integrare il criterio di imputazione oggettiva contemplato dall'articolo 5 del decreto 231 del 2001 in riferimento ai reati inclusi nel catalogo dei *predicate crime*[132].

Se fino a questo momento si è fatto riferimento alla commissione di un reato da parte di un algoritmo di intelligenza artificiale "tradizionale", il discorso si fa diverso quando ad integrare una fattispecie criminosa sia uno dei c.d. «nuovi agenti»[133] i quali, per via dei connotati di autonomia ed imprevedibilità ontologica[134] che li caratterizzano, non possono implicare una responsabilità indiretta e vicaria in capo al soggetto che li ha programmato o alla persona fisica che se ne avvale per i suoi scopi[135].

Dal momento in cui risulta assai complesso predeterminare e prevedere il comportamento dei suddetti paradigmi tecnologici, non è

[132] Per approfondimento in merito al secondo criterio di imputazione necessario per ascrivere una responsabilità *ex crimine* nei confronti della persona giuridica, vale a dire quello soggettivo contemplato dagli articoli 6 e 7 del d.lgs 231/2001, si rimanda al paragrafo che segue

[133] Cfr. SEVERINO, *Intelligenza artificiale e diritto penale*, in RUFFOLO (a cura di), *Intelligenza artificiale*, cit., 533.

[134] In argomento v. PIERGALLINI, *Intelligenza artificiale:da 'mezzo' ad 'autore' del reato?* cit., 97.

[135] V. BORSARI, *Intelligenza artificiale e responsabilità penale: prime considerazioni*, cit., 264 s.,

agevole individuare una persona umana cui muovere un rimprovero per colpa in relazione ad un fatto di reato verificatosi a causa di un inadempimento della macchina.

Sono pertanto due le soluzioni prospettabili nel caso di specie, entrambe meritevoli di un approfondimento specifico. La prima consiste nel considerare i *software* di IA come "soggetti di diritto", pertanto destinatari sia di garanzie che di sanzioni[136]. Ne consegue che in presenza di un reato cagionato dal malfunzionamento degli stessi, questa prima teoria è portata ad attribuire una responsabilità diretta in capo ai nuovi paradigmi tecnologici[137].

Un simile approdo affonda le radici nell'orientamento volto a riconoscere una soggettività all'algoritmo di IA per l'attribuzione di una responsabilità civilistica, approccio contemplato dalla stessa Risoluzione del Parlamento europeo sulla robotica[138].

Quest'ultimo concepisce la macchina come un autonomo centro di interessi e di imputazione, idoneo a rispondere direttamente dei danni cagionati. La macchina subisce un vero e proprio processo di antropomorfizzazione, si richiede, a titolo esemplificativo, la presenza di un registro *ad hoc* per iscrivere le stesse, assegnando loro un numero identificativo che funga da pseudo carta di identità elettronica. Questo nuovo soggetto di diritto andrebbe affiancato altresì da un congruo fondo patrimoniale[139] affinché lo stesso sia in grado di adempiere autonomamente alle obbligazioni.

Se il suddetto approccio nasce nello specifico per configurare una responsabilità civilistica nei confronti dei paradigmi di intelligenza artificiale, senza estendere i propri effetti in ambito penale, in realtà lo stesso

---

[136] Cfr. PIERGALLINI, *Intelligenza artificiale:da 'mezzo' ad 'autore' del reato?* cit., 101.

[137] Sul punto v. SEVERINO, *Intelligenza artificiale e diritto penale*, in RUFFOLO (a cura di), *Intelligenza artificiale*, cit., 533.

[138] Si rimanda alla Risoluzione del Parlamento europeo del 16 febbraio 2017, recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica. *https://op.europa.eu/it/publication-detail/-/publication/13fd56d0-8a65-11e8-ac6a-01aa75ed71a1/language-it*

[139] Si tratta di un fondo costituito da versamenti da parte di soggetti intervenuti in fase di creazione e di utilizzo del *software*

ha rappresentato un primo *input* per lo sviluppo di teorie volte ad introdurre una responsabilità penale diretta da ascrivere alla macchina.

Hanno già preso piede una serie di linee di pensiero propense a riconoscere il *tool* quale possibile autore di reato[140]. Alcune delle stesse sostengono che non sia così impensabile attribuire una soggettività penale alla macchina[141], come gran parte della dottrina vuole far cedere. Questi ultimi sono dell'idea che le nozioni stesse di liberto arbitrio e soggettività penale siano da considerare come meri costrutti sociali che prescindono da caratteristiche biofisiche, basterebbe quindi convenire che anche i *software* siano in grado di delinquere per risolvere la questione[142].

In aggiunta, gli stessi sostengono di sposare le argomentazioni di chi, nei primi anni duemila, si è mostrato propenso ad introdurre una responsabilità dedicata alla persona giuridica[143], in ultimo contemplata nel d.lgs. 231/2001: gli stessi sono infatti convinti che, proprio come gli enti, le nuove tecnologie siano caratterizzate da "un'intrinseca capacità criminale"[144] idonea a giustificare l'introduzione di una responsabilità diretta nei loro confronti.

In realtà, il parallelismo prospettato da alcuni autori sembrerebbe non essere condivisibile in quanto le macchine intelligenti, a differenza delle persone giuridiche, non si compongono di persone fisiche che possano integrare una fattispecie criminosa nell'interesse o a vantaggio delle stesse. È per questa ragione che il criterio di imputazione soggettiva cucito addosso alla persona giuridica non sembra adattarsi alle diverse peculiarità ontologiche che caratterizzano la macchina.[145]

---

[140] In argomento v. HALLEVY, *The Criminal Liability of Articial Intelligence Entities. From ScienceFiction to Legal Social Control*, in *Akron. Intell. Prop.J*., 2010, 171 ss.

[141] Per un approfondimento sul punto v. BORSARI, *Intelligenza artificiale e responsabilità penale: prime considerazioni*, cit., 266.

[142] Cfr. PIERGALLINI, *Intelligenza artificiale:da 'mezzo' ad 'autore' del reato?* cit., 103 s.

[143] Sul punto v. CAPPELLINI, *Machina delinquere non potest? brevi appunti su intelligenza artificiale e responsabilità penale,* in *Discrimen*, 2019, 12 ss.

[144] V. SEVERINO, *Intelligenza artificiale e diritto penale*, in RUFFOLO (a cura di), *Intelligenza artificiale*, cit., 535

[145] Sul punto v. SEVERINO, *Intelligenza artificiale e diritto penale*, in RUFFOLO (a cura di), *Intelligenza artificiale*, cit., 535; CAPPELLINI, *Machina delinquere non potest*? cit., 13 ss.; PANATTONI, *Ai and criminal law: the myth of 'control' in a data-driven society*, cit., 131 s.

Sembrerebbe pertanto da escludere una rimproverabilità nei confronti di un algoritmo, il quale viene percepito dalla generalità dei consociati come incapace sia di rappresentarsi una fattispecie criminosa e volerne la realizzazione concreta che di porre in essere un comportamento negligente, imprudente o carente di perizia[146].

Se risultano esserci notevoli perplessità in relazione alla prima soluzione pocanzi illustrata, decisamente più condivisibile sembra essere il secondo espediente giuridico prospettato da autorevole dottrina. Quest'ultima, infatti, non rinnegando i notevoli benefici che derivano dall'impiego delle nuove tecnologie a supporto della *compliance*, suggerisce al legislatore di definire un'area di rischio consentito[147] da ricondurre all'operato della tecnologia. È nel caso in cui si fuoriesca dall'area "tollerabile" che le irregolarità e le violazioni realizzate dal *tool* implicheranno una responsabilità in capo alla persona fisica che ha programmato il *software*, dando luogo ad una rimproverabilità a titolo di colpa o di dolo eventuale a seconda della gravità del caso specifico[148].

Una soluzione di questo tipo sembrerebbe idonea ad attenuare le forti perplessità connesse al riconoscimento di una responsabilità diretta in capo alla persona fisica qualora ad integrare una fattispecie criminosa sia stato un *tool* capace di decidere in manera autonoma e svincolata dal programmatore o dall'utilizzatore dello stesso. In questi casi, infatti, risulta particolarmente ostico riconoscere un profilo di colpevolezza nei confronti della persona fisica senza scadere in forme di responsabilità penale oggettiva considerate costituzionalmente illegittime nel nostro ordinamento. Difficoltà confermate altresì dal *modus operandi* delle nuove tecnologie, basato su reti ed interazioni tra una moltitudine di soggetti, il quale non consente

[146] Sul punto v. CAPPELLINI, *Machina delinquere non potest? brevi appunti su intelligenza artificiale e responsabilità penale,* in *Discrimen*, 2019, 15 ss; PANATTONI, *Ai and criminal law: the myth of 'control' in a data-driven society*, cit., 130 s.

[147] Il rischio è da considerarsi consentito quando a fianco dello stesso si verificano altresì dei benefici, sul punto v. YATES, *Paura e società del rischio. Un'intervista a Urlich Beck*, in *Lo Sguardo*, 2016, II, 213.

[148] In argomento v. PIERGALLINI, *Intelligenza artificiale:da 'mezzo' ad 'autore' del reato?* cit., 88.; SEVERINO, *Intelligenza artificiale e diritto penale*, in RUFFOLO (a cura di), *Intelligenza artificiale*, cit., 535

facilmente di rintracciare una persona fisica alla quale riconoscere una responsabilità criminosa[149].

Per concludere, dal momento in cui sembra opportuno escludere una responsabilità penale diretta in capo al paradigma di intelligenza artificiale, sia nel caso in cui lo stesso presenti ancora importanti margini di dipendenza dalla persona fisica che lo ha programmato che nell'eventualità in cui quest'ultimo sia totalmente indipendente da ogni contributo umano, la soluzione meglio rispondente alle caratteristiche fondamentali proprie del diritto penale in vigore nel nostro ordinamento consiste nell'attribuire una responsabilità, alle specifiche e stringenti condizioni prima evidenziate, in capo al soggetto che ha avuto l'onere di configurare un *tool* o che si avvalga dello stesso nel compimento delle attività.

Nella prima eventualità, infatti, un'inesattezza della macchina corrisponderebbe ad un errore di programmazione o ad un utilizzo improprio della stessa, nella seconda circostanza invece, il programmatore o l'utilizzatore sarebbero rimproverabili nel caso in *l'algorithm misconduct* produca effetti negativi che si estendano oltre l'area di rischio consentito che deve però essere previamente fissata dal legislatore.

4. La colpa di organizzazione in presenza di un *algoritmic misconduct*

Nel modello di responsabilità dedicato alle persone giuridiche delineato dal decreto legislativo 231 del 2001, a differenza di quanto si verifica nei sistemi giuridici anglosassoni basati sulla *vicarious liability* o sull'*identification theory*, non basta la sola integrazione del primo criterio oggettivo di imputazione per ritenere l'ente responsabile del reato presupposto verificatosi al suo interno. Il legislatore del 2001 ha infatti previsto un secondo livello di ascrizione della responsabilità, quello soggettivo, il quale trova una puntuale disciplina negli articoli 6 e 7 del

[149] Cfr. PANATTONI, *Ai and criminal law: the myth of 'control' in a data-driven society*, cit., 137.

decreto a seconda della qualifica rivestita dal soggetto arrivo, apicale nel primo caso e sottoposto nel secondo.

Nell'ordinamento italiano, pertanto, non si condanna l'ente per il solo fatto che un soggetto appartenente al suo organico abbia integrato una fattispecie criminosa nel suo interesse o a suo vantaggio ma si richiede altresì una forma di colpevolezza in capo alla *corporation*. La scelta è stata quella di delineare una tipologia di colpa *ad hoc* per la persona giuridica, a carattere squisitamente normativo, la quale si sostanzia in un *deficit* organizzativo[150]. Quel che si rimprovera all'ente, infatti, è la mancata adozione e l'inefficace attuazione dell'insieme dei presidi normativi idonei a prevenire i reati elencati nel decreto in esame e quindi la sua scelta di aver accettato che un soggetto appartenente all'azienda integrasse una fattispecie criminosa [151].

La c.d. colpa di organizzazione si configura diversamente a seconda che a delinquere sia stato un soggetto apicale o un sottoposto. Se in questo secondo caso la colpevolezza dell'ente si traduce in una carenza in termini di controllo nei confronti dell'operato del dipendente, nel caso in cui il reato sia stato commesso da un apicale[152], è meno immediato scorgere una vera e propria colpa di organizzazione in capo all'ente in quanto il reato compiuto dagli amministratori o dai direttori generali, in virtù della teoria dell'immedesimazione organica, è reato dell'ente.

In realtà, anche in questa seconda ipotesi, sussiste la possibilità in capo alla persona giuridica di dissociarsi dall'operato dei suoi vertici adottando un modello organizzativo idoneo, tanto che la scelta di organizzarsi va considerata come un temperamento alla suddetta teoria, tale da escludere l'automatica sovrapposizione tra le condotte illecite degli apicali e la politica d'impresa.

Una volta chiarito in cosa consiste il criterio di imputazione soggettiva, è bene porsi il medesimo interrogativo già esplicitato in

[150] In argomento v. MONGILLO, *Presente e futuro della compliance penale*, cit., 3 ss.
[151] Per un approfondimento sul punto v. DI GIOVINE, *Il criterio di imputazione soggettiva*, in LATTANZI, SEVERINO (*a cura di), La responsabilità da reato degli enti*, cit.,, 203 ss.
[152] Questa ipotesi è disciplinata dall'articolo 6 del d.lgs. 231 del 2001

relazione al primo livello di ascrizione della responsabilità, vale a dire, come conciliare lo stesso con la circostanza per cui il verificarsi di una fattispecie criminosa sia dovuta al malfunzionamento di un *tool* di intelligenza artificiale.

In un ordinamento come quello italiano dove la responsabilità ascriviibile all'ente non si fonda solo sul criterio oggettivo ma richiede altresì una colpa di organizzazione, risulta particolarmente complesso concludere che sussista una vera e propria "colpa" in capo alla persona giuridica al configurarsi di un errore del *software*.

La verificazione di un *algorithm misconduct*, pertanto, non può determinare *sic et simpliciter* una responsabilità penale in capo alla persona giuridica in quanto, unitamente agli altri requisiti giuridici, occorre dimostrare che l'ente non abbia predisposto dei presidi organizzativi quali, ad esempio, una serie di procedure interne volte a valutare l'*output* algoritmico idonei a consentire all'ente di discostarsi dallo stesso se considerato inattendibile o viziato[153].

Nel caso in cui l'ente abbia adottato ed efficacemente attuato un modello di *compliance* ben strutturato e idoneo a gestire gli eventuali *bias* in cui può incorrere l'algoritmo di cui ci si avvale, facendo sostanzialmente del suo meglio per garantire un'attività di prevenzione razionale e accurata, sembra opportuno concludere che non sussista alcuna colpa di organizzazione e, di conseguenza, nessuna responsabilità penale può essere ascritta all'ente.

Un modo *de iure condendo* per attestare sussistenza del criterio soggettivo contemplato dagli articoli 6 e 7 del d.lgs 231/2001 sarebbe quello di annoverare l'impiego dei nuovi paradigmi tecnologici nel compendio delle *best practices* delineate dagli organismi di settore a cui l'ente deve conformarsi per la predisposizione di un modello organizzativo efficace nel prevenire i reati presupposto elencati dallo stesso[154], al fine di positivizzare le cautele richieste alle *corporation*.

[153] In argomento v. SABIA, *Artificial intelligence and environmental criminal Compliance*, cit., 186 ss.
[154] Sul punto v. NISCO, *Riflessi della compliance digitale in ambito 231*, cit. 10 s.

In questo modo, sia il mancato ricorso a paradigmi tecnologici a supporto della *compliance* che la mancata previsione di un insieme di controlli che attestino il corretto funzionamento degli stessi, potrebbe comportare un giudizio negativo da parte dei giudici chiamati a valutare l'idoneità dei presidi organizzativi adottati dall'ente, con la conseguente attestazione di un deficit organizzativo in capo allo stesso sintomatico della presenza di una colpa di organizzazione.

Le conclusioni a cui si è giunti fino a questo momento risultano valide qualora venga impiegato un paradigma tecnologico che funga da mero supporto all'attività delle persone fisiche preposte e che sia sostanzialmente controllabile da parte delle stesse, tale per cui è possibile riconoscere una responsabilità in capo a queste ultime.

Il discorso, tuttavia, è diverso quando ad essere utilizzati in ambito *criminal compliance* siano algoritmi di intelligenza artificiale capaci di prendere decisioni in piena indipendenza e autonomia rispetto ad apicali e sottoposti. In quest'ultimo caso, risulta impossibile estendere una responsabilità *ex crimine* all'ente in quanto manca del tutto un reato presupposto che contempli la macchina quale soggetto attivo di una fattispecie criminosa.

Per fornire una soluzione alla suddetta situazione di fatto, parte della dottrina[155] ha avanzato due proposte ben precise. La prima consiste nell'introduzione di nuovi reati commessi direttamente dalle nuove tecnologie, per poi annoverare gli stessi nell'elenco di fattispecie criminose contemplate dagli articoli 24 ss. d.lgs. 231/2001.

La seconda si sostanzia nell'introduzione di una responsabilità autonoma in capo all'ente poiché prescindente dalla necessità di integrare il primo criterio di imputazione oggettiva, vale a dire la commissione di un reato tassativamente enumerato nel decreto 231/2001 da parte di un apicale o un sottoposto, nell'interesse o a vantaggio dell'ente.

[155] In argomento v. PANATTONI, *Ai and criminal law: the myth of 'control' in a data-driven society*, cit., 137 ss.

Secondo gli autori della suddetta soluzione, la responsabilità ascrivibile alla persona giuridica dovrebbe basarsi sul mancato rispetto, da parte della stessa, di un compendio di obblighi giuridici orientati a garantire il corretto utilizzo dei paradigmi di IA, omissione che ha reso l'ente incapace di prevenire il rischio di verificazione di reati dovuti al malfunzionamento del paradigma tecnologico.

Una soluzione di questo tipo, per essere congruamente implementata in un ordinamento come quello vigente nel nostro Paese, innervato alla filosofia della *compliance*, richiederebbe un previo intervento normativo volto, *in primis*, ad introdurre una disciplina *ad hoc* in materia di nuove tecnologie che contempli altresì gli adempimenti che si rendono necessari per un congruo utilizzo delle stesse, e, in secondo luogo, orientato a disciplinare un'area d rischio consentito quale esito del bilanciamento tra opportunità e rischi derivanti dalla *digital criminal complinace.*

5. Responsabilità degli enti e controlli a distanza

L'utilizzo dei nuovi paradigmi tecnologici a supporto della *compliance* dell'ente per la conduzione di attività di mappatura del rischio reato, per la procedimentalizzazione delle attività interne, per la gestione dei flussi finanziari nonché per il monitoraggio dei flussi informativi, implica che una delle gran parte delle attività ricomprese in quest'ambito ricadano nella categoria dei controlli predisposi dall'ente nei confronti dei soggetti appartenenti all'azienda. Questi ultimi consistono principalmente nell' accesso alle *e-mail*, nel monitoraggio delle conversazioni e nel controllo in merito all'utilizzo del potere di spesa, ma rischiano di sfociare altresì in una vera e propria attività di profilazione del lavoratore quando ci si avvale delle tecniche di *Big data analysis* per calcolare il tasso di propensione al rischio di uno specifico individuo.

Nel nostro ordinamento sussiste una specifica disciplina volta a tutelare i lavoratori dai c.d. controlli a distanza. Quest'ultima, se prima della riforma entrata in vigore nel 2015 si estrinsecava nel solo articolo 4 dello

Statuto dei Lavoratori, ad oggi si basa sullo stesso articolo 4, il quale ha subito una riformulazione sostanziale, nonché sugli articoli 38 dello Statuto dei lavoratori e 171 del Codice Privacy.

La riforma del 2015 si è resa necessaria per tre ordini di motivi, in primo luogo per aggiornare la disciplina alla luce delle innovazioni tecnologiche che hanno interessato anche il mondo del lavoro, in secondo luogo per annoverare tra le esigenze che legittimano i controlli a distanza la tutela del patrimonio aziendale, in terzo luogo per introdurre una disciplina riguardo l'impiego delle informazioni registrate nello svolgimento delle diverse attività di controllo[156].

L'articolo 4 dello statuto dei lavoratori, ad oggi rubricato "Impianti audiovisivi e altri strumenti di controllo", al comma 1 stabilisce che questi ultimi possano essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale. La disposizione normativa in questione impone inoltre che gli stessi possano essere istallati solo previo accordo con le rappresentanze sindacali e gli altri organismi tassativamente elencati dalla disposizione in esame[157].

La principale innovazione introdotta dalla riforma del 2015 consiste nell'inclusione degli "altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori", dove per "distanza" si intende sia quella fisica, con riferimento, ad esempio, all'utilizzo di telecamere per monitorare da lontano un determinato soggetto, che quella cronologica, come nel caso dei controlli che abbiano ad oggetto le attività non verificatesi contestualmente allo svolgimento dell'attività lavorativa[158].

È nel comma 2 del medesimo articolo 4 che vengono disciplinati i casi in cui i profili procedurali contemplati dal comma 1 possono essere

[156] Sul punto v. NISCO, *Prospettive penalistiche del controllo a distanza sull'attività lavorativa nell'attuale contesto normativo e tecnologico*, in *Riv. Trim. Dir. Cont. Pen*, 2021, 90 s.
[157] Si fa riferimento all'autorizzazione che deve essere concessa dalla sede territoriale dell'ispettorato del lavoro
[158] Cfr. Cassazione civile, sez. lav., n. 1236 del 18 febbraio 1983. In argomento v. Martinelli, *Il controllo a distanza del lavoratore e nuove tecnologie*, in *Ciberspazio e diritto*, 2015, 359; NISCO, *Prospettive penalistiche del controllo a distanza sull'attività Lavorativa*, cit., 89 s.

disattesi, tanto che in relazione alle stesse non si richiedono le autorizzazioni sopra illustrate. I casi di esenzione sono due e fanno riferimento all'utilizzo degli strumenti che servono al lavoratore per porre in essere la prestazione lavorativa nonché gli strumenti volti a registrare gli accessi e le presenze.

Sul punto si rende doverosa una precisazione. Il termine "strumento" è così generico da poter includere sia la componente *hardware* che *software*. Pertanto, il *computer* utilizzato dal lavoratore nello svolgimento dell'attività lavorativa, alla luce della sua destinazione, merita di essere ricompreso nella disciplina dettata dal comma 2 dell'articolo 4 St. lav., ma lo stesso ragionamento non può estendersi in automatico ai programmi e alle applicazioni istallate nel suddetto *hardware*. Queste ultime saranno infatti oggetto di un'autonoma attività di valutazione che attesti la loro destinazione a strumenti "anche di"[159] controllo o la valenza di mezzi esclusivamente idonei allo svolgimento della prestazione lavorativa, con conseguente applicazione del comma 1 nel primo caso e del comma 2 in relazione alla seconda ipotesi[160].

Quanto all'articolo 171 del *Codice privacy*, quest'ultimo prevede che una violazione delle disposizioni di cui all'articolo 4, comma 1, St. Lav. venga punita con le sanzioni contemplate dall'articolo 38 del medesimo testo normativo, il quale contempla l'irrogazione della sanzione dell'ammenda o dell'arresto da 15 giorni ad un anno, salvo i casi connotati da maggiore gravità.

È bene ora interrogarsi se sussista una responsabilità in capo all'ente qualora lo stesso ponga in essere una violazione della disciplina dei controlli interni pocanzi delineata. Dal momento in cui li reato previsto dall'articolo 171 del Codice Privacy non viene contemplato tra i reati presupposto elencati dagli articoli 24 e seguenti del d.lgs. 231/2001, è da escludere che l'integrazione dello stesso comporti una responsabilità in capo alla persona giuridica in quanto quest'ultima viene a configurarsi nei soli casi in cui sia

[159] V. art. 4 St. Lav.

[160] Per fare un esempio sul punto, l'installazione di un'applicazione finalizzata al controllo degli accessi effettuati dal lavoratore ai diversi siti web, come nel caso di *Clever Control*, ricadrà nella formulazione efferata dal comma 1 dell'art. St. Lav. e le autorizzazioni dallo stesso contemplate.

stato posto in essere un reato tassativamente menzionato dal decreto, da parte di un apicale o sottoposto, nell'interesse o a vantaggio dell'ente[161].

L'unica ipotesi in cui la persona giuridica possa essere considerata responsabile consiste nella circostanza tale per cui l'attività di controllo esercitata sui lavoratori sia idonea ad integrare uno dei reati contro la *privacy*[162] menzionati esplicitamente dall'articolo 24 bis d.lgs. 231/2001.

Se è da escludere la configurazione di profili di responsabilità penale ascrivibili alla persona giuridica, ad eccezione del caso pocanzi illustrato, lo stesso non po' dirsi in merito alla verificazione di una responsabilità a carattere amministrativo. L'articolo 114 del Codice Privacy, infatti, richiama la disciplina contenuta nell'art. 4 della legge 20 maggio 1970, n. 300 e si configura quale norma nazionale di maggior tutela ai sensi di quanto stabilito dall'articolo 88 GDPR che si occupa di disciplinare il trattamento dei dati nel contesto lavorativo.

La mancata inclusione dell'articolo 117 Codice Privacy tra il novero dei reati presupposto e, più in generale, l'assenza di una disciplina volta a coniugare l'esigenza in capo all'ente di predisporre un modello organizzativo con l'altrettanto valida necessità di rispettare la disciplina sui controlli difensivi introdotta a garanza dei lavoratori, vengono a configurarsi come dei vuoti normativi da colmare al più presto attraverso un intervento normativo da parte del legislatore[163]. Necessità che si fa tanto più impellente se si considera che il progressivo sviluppo tecnologico comporta l'introduzione di strumenti che consentono un controllo sempre più incisivo del lavoratore[164].

Nonostante l'impossibilità di ascrivere una responsabilità *ex crimine* nei confronti dell'ente in caso di violazione della disciplina dedicata ai controlli interni, salvo i casi in cui si verifichi un reato che attenti al diritto

[161] Sul punto v. NISCO, *Prospettive penalistiche del controllo a distanza sull'attività Lavorativa*, cit., 103 s.
[162] Si fa riferimento alle fattispecie criminose contemplate dagli Artt. 615-ter, 615-quater, 615-quinquies, 617-quater, 617-quinquies c.p., richiamati – insieme ad altri – dall'art. 24-bis d.lgs. 231/2001.
[163] Di quest'opinione NISCO, *Prospettive penalistiche del controllo a distanza sull'attività Lavorativa*, cit., 104.
[164] Basti pensare all'utilizzo delle tecnologie *blockchain* o ai paradigmi di *Big data analysis*

alla *privacy* del lavoratore, quest'ultima può essere validamente considerata come un argine alla *digital criminal compliance*, uno strumento idoneo a valutare la legittimità dell'impiego dei nuovi paradigmi automatici a supporto dei controlli contemplati dal modello, dal momento in cui un utilizzo improprio degli stessi comporta la possibile contestazione di condotte penalmente rilevanti non a discapito della persona giuridica ma nei confronti del datore di lavoro persona fisica[165].

La situazione giudica vigente delinea profili di profonda incoerenza. Il nostro ordinamento, infatti, prescrive ai *board* delle imprese di impegnarsi nel predisporre un apparato organizzativo capace di prevenire i reati presupposto in azienda, ma allo stesso tempo espone lo stesso al rischio di incorrere in una responsabilità penale per la violazione degli articoli 171 Codice Privacy, 4 e 38 St. Lav., disposizioni elaborate dal legislatore non per disciplinare le attività di *compliance* ed *internal investgation* dell'ente, ma per tutelare tutt'altri beni giuridici[166].

Non si può non evidenziare il conflitto di interessi che viene in rilievo sul punto e che vede contrapporre da un lato, il diritto del lavoratore a non essere vittima di controlli indebiti, dall'altro, il diritto in capo al datore di lavoro di mantenere la segretezza delle attività di investigazione poste in essere in azienda onde minarne l'efficacia e, più in generale, la sua pretesa di esercitare liberamente i controlli prescritti dal d.lgs. 231/2001 per prevenire la commissione di reati in azienda.

Questa divergenza di interessi ha dato adito ad una pratica che risulta diffusa nella prassi, vale a dire quella della c.d. sorveglianza occulta[167]. In molti casi il datore di lavoro predispone un'attività di controllo senza rispettare previamente le condizioni contemplate al comma 1 dell'art. 4 St. Lav., adducendo come motivazione che giustifichi questa omissione la presenza di indizi di reato.

---

[165] Sul punto v. BIRRITTERI, *Controllo a distanza del lavoratore e rischio penale*, in *Sist. Pen*., 2021, 4 s.

[166] In argomento v. BIRRITTERI, *Controllo a distanza del lavoratore,* cit., 5 s.

[167] V. BIRRITTERI, *Controllo a distanza del lavoratore,* cit., 4; GULLO, *Compliance*, cit., 15.

I controlli difensivi in senso stretto, infatti, vale a dire quelli esercitati con l'obiettivo di accertare la sussistenza di una condotta illecita di cui si presume, in basi ad indizi concreti[168], siano autori i singoli dipendenti e in un momento precedente all'avvio di un procedimento penale, sembrerebbero collocarsi al di fuori dell'ambito applicativo dell'articolo 4 St. Lav. anche se condotti nel corso dell'attività lavorativa dei sottoposti. Pertanto, per essere legittimi, non richiedono un previo accordo con l'autorità sindacale o, in mancanza, l'autorizzazione da parte della sede locale dell'ispettorato del lavoro, come precisato da gran parte della giurisprudenza di legittimità espressasi sul punto[169].

Su questi temi si è pronunciata più volte la Corte EDU con l'obiettivo di stabilire dei principi di diritto generalmente applicabili[170].

La prima sentenza meritevole di essere menzionata è quella pronunciata all'esito della vicenda Barbulescu[171]. Nel caso di specie i giudici di Strasburgo hanno decretato la legittimità dell'attività di sorveglianza occulta qualora la stessa sia necessaria e finalizzata al raggiungimento di uno scopo specifico e consentito e sia svolta in maniera proporzionata rispetto all'obiettivo che si intende perseguire.

È sulla scia di quanto delineato dall'autorevole precedente giurisprudenziale pocanzi menzionato che si è posta la seconda pronuncia della Corte EDU, quella relativa al caso Lopez Ribalta[172]. In quest'occasione i giudici di Strasburgo hanno ritenuto ammissibile l'installazione di telecamere nascoste sul luogo di lavoro, con conseguente

---

[168] In presenza, ad esempio, di una segnalazione interna ex art. 6, comma 2-bis d.lgs. 231/2001, meglio nota come *whistleblowing*.

[169] V. Cassazione civile sez. lav. 03 aprile 2002 n. 4746; Cassazione civile sez. lav. 17 luglio 2007 n. 15892; Cassazione civile sez. lav. 23 febbraio 2010 n. 4375; Cassazione civile sez. lav. 23 febbraio 2012 n. 2722; Cassazione civile sez. lav. 8 novembre 2016 n. 22662 In argomento v. FALSONE, *L'infelice giurisprudenza in materia di controlli occulti e le prospettive del suo superamento*, in *Riv. It. Dir. Lav.*, 2015, 984 ss.; In argomento v. MARTINELLI, *Il controllo a distanza del lavoratore e nuove tecnologie*, cit., 360 ss.; CAPOBIANCO, *Privacy e controlli a distanza :ultimi approdi normativi e giurisprudenziali*, in *SalvisJuribus*, 2018, 8 s.

[170] D'APONTE, *I controlli a distanza e la videosorveglianza nei luoghi di lavoro tra diritto nazionale e giurisprudenza CEDU*, in *Rivista giuridica del lavoro e della previdenza sociale*, 2020, 238 ss.; BIRRITTERI, *Controllo a distanza del lavoratore*, cit., 4 ss.

[171] Cfr. Corte EDU, Bărbulescu v. Romania, 12 gennaio 2016, sez. IV, ricorso n. 61496/08, su *https://hudoc.echr.coe.int/*

[172] V. Corte EDU, Grande Camera, Lopez Ribalda e altri c. Spagna, 17 ottobre 2019.

mancata violazione dell'art. 8 CEDU, in quanto vi erano fondati e ragionevoli sospetti di furti commessi dai lavoratori ai danni del patrimonio aziendale, l'area oggetto di ripresa era circoscritta, le operazioni sono state condotte per un limitato periodo di tempo e non risultava possibile ricorrere ad altri mezzi meno invasivi.

La Corte, pertanto, ha affermato il seguente principio di diritto: i controlli occulti posti in essere dal datore di lavoro senza aver osservato la disciplina in materia sono legittimi in presenta di tre elementi indefettibili quali l'emersione di concreti indizi di reati in un momento precedente agli stessi, la proporzionalità nell'esercizio delle operazioni[173] e, infine, l'interruzione della suddetta sorveglianza occulta una volta terminata l'indagine[174].

A fronte dei persistenti dubbi in materia, è utile ribadire la necessità di un intervento da parte del legislatore sul punto, volto a conciliare la disciplina in materia di *criminal compliance* e *internal investigations* contemplata dal d.lgs. 231/2001 e quella relativa ai controlli interni ex art 4 St. Lav, 171 Codice Privacy e 38 St Lav., così da coniugare l'esigenza in capo all'ente di predisporre un modello organizzativo efficace con l'altrettanto valida necessità di rispettare i diritti dei lavoratori.

[173] I controlli devono limitarsi ad accertare la verificazione di un illecito
[174] In argomento BIRRITTERI, *Controllo a distanza del lavoratore,* cit., 5 s.

CONCLUSIONI

Preso atto del ruolo di assoluta centralità rivestito dai modelli organizzativi in quanto concretizzazione dalla *compliance* penale, nonché della scarsità di pronunce giudiziali volte ad attestarne l'idoneità, emerge, a oltre vent'anni dall'introduzione della responsabilità *ex crimine* delle persone giuridiche nel nostro Paese, la necessità di un intervento da parte del legislatore volto a chiarire gli adempimenti che si reputano necessari per la costruzione di un MOG idoneo a prevenire i c.d. reati presupposto. Al netto della recente "svolta" segnata dalla sentenza Impregilo, le indicazioni contenute sul punto nel decreto legislativo 231 appaiono, infatti, piuttosto scarne, non del tutto capaci di guidare pedissequamente l'ente nelle operazioni di *compliance* e sempre bisognose di essere affiancate dalle linee guida elaborate dalle principali autorità di settore.

Per le ragioni sopra delineate, si rende doverosa un'opera di positivizzazione delle diverse cautele che si richiede agli enti di osservare nella predisposizione delle misure organizzative interne, incardinando le indicazioni contenute nelle *best practices* in un unico testo normativo, così da garantire una maggiore certezza del diritto e fornire alla magistratura dei parametri oggettivi su cui fondare il giudizio di idoneità dei modelli organizzativi.

L'analisi svolta finora testimonia quanto sia vantaggioso avvalersi dei nuovi paradigmi tecnologici a supporto della *compliance* penale e nelle attività di predisposizione di un modello organizzativo idoneo *ex* art. 6 co. 2 d.lgs. 231/2001.

La digitalizzazione della maggior parte delle operazioni di *compliance* può consentire spesso una migliore gestione della complessità interna ed esterna all'impresa, una maggiore efficacia ed efficienza nell'esercizio delle operazioni tipiche, un incremento dell'attitudine preventiva del modello nonché un risparmio di spesa, con conseguente migliore allocazione delle limitate risorse di cui dispone la persona giuridica.

È per i seguenti motivi che appare opportuno valutare l'inclusione, tra gli adempimenti da incardinare in un futuro progetto di riforma incentrato sui modelli organizzativi, l'utilizzo dei nuovi paradigmi tecnologici nell'esercizio delle operazioni che caratterizzano gli stessi, seppur nel rispetto di condizioni ben precise

volte ridimensionare il rischio di incorrere in *bias* nonché in violazioni di diritti fondamentali.

Per scongiurare l'effetto "*black box*" e la produzione di *output* viziati a causa dell'impiego di dati inattendibili, bisognerebbe favorire l'uso dei *software* a supporto della *compliance* che abbiano conseguito le certificazioni ISO/IEC volte ad attestare la qualità dei *big data* quali *input* di ogni algoritmo di intelligenza artificiale nonché l'attendibilità dei *software* di cui l'ente intende avvalersi.

In aggiunta, per evitare che i *tools* "intelligenti" producano dei risultati capaci di dare seguito ad una violazione dei diritti umani incardinati nella Convezione europea dei diritti dell'uomo, si rende necessario che le imprese predispongano un "controllo umano significativo"[175] volto ad accertare che i paradigmi di intelligenza artificiale adottati dalla *corporation* siano rispettosi dei principi contemplati dalla Carta Etica Europea, delle indicazioni contenute nel Libro bianco sull'intelligenza artificiale e, non appena entrate in vigore, delle regole incardinate nella proposta di regolamento europeo sull'intelligenza artificiale, meglio noto come *AI act*.

Al fine di incentivare l'ente ad organizzarsi *ex ante* e non solo in un momento successivo alla verificazione della fattispecie criminosa, come tendono a fare gran parte delle PMI, si potrebbero prospettare delle misure premiali specifiche per l'ente che sin da subito sceglie di adottare un modello organizzativo in *compliance* con le disposizioni legislative in vigore e nel rispetto dei nuovi requisiti oggetto di auspicabile riforma. Benefici che potrebbero variamente modularsi, fermo restando che un giudizio in merito all'esclusione da ogni forma di responsabilità dovrebbe restare di competenza della sola autorità giudiziaria.

Una volta inserito l'impiego dei nuovi paradigmi digitali tra gli adempimenti volti a consentire la predisposizione di un MOG idoneo, appare necessario interrogarsi, in prospettiva evolutiva, sui profili di responsabilità degli amministratori e degli enti in presenza di un *algorithmic misconduct.*

A legislazione vigente e sussistendone tutti i relativi presupposti, rimane sempre possibile attribuire una responsabilità in capo agli operatori che si sono avvalsi di *software* nella conduzione delle operazioni di *compliance* qualora si tratti

[175] Cfr. UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, cit., 77.

di paradigmi digitali che presentato un elevato grado di dipendenza dalla persona fisica.

Come si è visto durante la trattazione, invece, appare complesso pervenire al medesimo risultato qualora si faccia riferimento a strumenti digitali pienamente autonomi sia nel ricavare gli *input* che nel perfezionare il proprio operato sulla base dell'esperienza concreta, con esiti, dunque, per definizione imprevedibili. In questo secondo caso, concordemente con quanto prospettato da parte della dottrina, andrebbe dapprima operato, con una specifica regolamentazione legislativa, un bilanciamento tra i benefici ed i rischi derivanti dall'utilizzo dei *tools* "intelligenti", per poi delineare una soglia di rischio consentito al superamento della quale ricondurre dei profili di responsabilità in capo alle persone fisiche che hanno deciso di avvalersi comunque dei paradigmi di intelligenza artificiale.

BIBLIOGRAFIA

ACCINNI, *L'utilizzo criminogeno della blockchain: gli smart contract*, in *Sist. pen.*, 2022, 130;

ALESSANDRI, SEMINARA, *Diritto penale commerciale, vol. I, Principi generali*, Torino, 2018;

ALESSANDRI, *Note penalistiche sulla nuova responsabilità delle persone giuridiche*, in *Riv. Trim. dir. pen. econ.*, 2002, 30;

ALESSANDRI, *Diritto penale e attività economiche*, Bologna, 2010;

AMORE, "*Fairness", "Transparency" e "Accountability" nella protezione dei dati personali*, in *Studium iuris*, 2020, 400;

AMRAM, *The Role of the GDPR in Designing the European Strategy on Artificial Intelligence: Law-Making Potentialities of a Recurrent Synecdoche*, in *Opinio Juris in Comparatione*, 2020, 60;

ARDUINI, *La "scatola nera" della decisione giudiziaria: tra giudizio umano e giudizio algoritmico*, in *BioLaw Jurnal*, 2021, 420;

ARENA, *La responsabilità amministrativa delle imprese: il d.lgs. n. 231/2001: Normativa, Modelli organizzativi, temi d'attualità*, in *Nuova Giuridica*, 148;

ARLEN, BUELL, *L'importanza della regolamentazione delle indagini interne nella giustizia negoziate degli enti*, in CENTONZE, GIAVAZZI («a cura di») *Internal Investigations, best practices e istanze di regolamentazione*, Torino, 2021, 1;

ARNER, BARBERIS, BUCKLEY, *FinTech, RegTech and the Reconceptualization of Financial Regulation, in Northwestern Journal of International Law & Business*, Hong Kong, 2016, 1;

AVANZINI, *Decisioni amministrative e algoritmi informatici. Predeterminazione analisi predittiva e nuove forme di intellegibilità*, Napoli, 2020;

BAMBERGER, *Tecnologies of compliance: risk and regulation in a digital age*, in *Texas law review*, 2010;

BARATTELLI, *Giustizia predittiva, decisione robotica e ruolo del giudice*, in Giust. Civ., 2020, 265;

BARBARO, *Cepej, adottata la prima Carta etica europea sull'uso dell'intelligenza artificiale (AI) nei sistemi giudiziari*, in *Questione giustizia*, 2018, 1;

BARILLARO, *Che cos'è un algoritmo in generale e in informatica,* in *Informatica per tutti*, 2023, 1;

BARRY, LIBERT, *Why Boards Must Embrace Big Data*, in *NACD Directorship*, 2013, 1;

BARTOLI, *Il criterio di imputazione oggettiva*, in Lattanzi, Severino (*a cura di), La responsabilità da reato degli enti*, vol. I, Torino, 2021, 152;

BARTOLOMUCCI, *L'adeguatezza del Modello nel disposto del d.lgs. 231 e nell'apprezzamento giudiziale. Riflessioni sulla sentenza d'appello "Impregilo"*, in *Resp. amm. soc. ed enti*, 2012, 155;

BARTOLOMUCCI, *Ribadita dalla S.C. la centralità dell'art. 6, d.lgs. n. 231/2001 nella valutazione giudiziale della idoneità ed effettività del modello*, in *Resp. amm. soc. ed enti*, 2014, n. 2, 250;

BASILE, *Intelligenza artificiale e diritto penale: quattro possibili percorsi d'indagine*, in *Dir. Pen e Uomo*, 2022, 1;

BASSI, MORELLI, *Internal Investigations: uno strumento di monitoraggio e governo del rischio nell'ottica dell'efficacie attuazione del modello organizzativo*, in *La resp. amm. soc. e enti*, 2019, 4, 280;

BAZZERLA, *La gestione della complessità e il controllo di gestione in azienda,* in *Metodi e strumenti controllo di gestione*, 2018, 1;

BERMAN, HAFNER, *The Potential of AI to Help Solve the Crisis in our Legal System,* in *CACM*, vol.32(8), 1989;

BEVILACQUA, *Le varie tipologie di blockchain*, in BATTAGLINI, GIORDANO (a cura di), *Blockchain e smart contracts*, Milano, 2019;

BIANCHI, *Investire attraverso i security token, entro il 2023*, in *CETIF*, 2022, 1;

BIRRITTERI, *Big Data Analytics e compliance anticorruzione. Profli problematici delle attuali prassi applicative e scenari futuri*, in *Riv. Trim. Dir. Pen. Cont*., 2019, 289;

BIRRITTERI, *Controllo a distanza del lavoratore e rischio penale*, in *Sist. Pen*., 2021, 1;

BODEI, *Dominio e sottomissione. Schiavi, animali, macchine e intelligenza artificiale*, Bologna, 2019;

BORGOBELLO, *Sentenza Impregilo: metodi di valutazione di adeguatezza del modello organizzativo, dei poteri dell'Organismo di vigilanza e della condotta fraudolenta degli amministratori*, in *Giurisprudenza Penale*, 2022, 1;

BORSARI, *Intelligenza artificiale e responsabilità penale: prime considerazioni*, in *MediaLaws*, 2019, 260;

BORTOLOTTO, *In G.U. il d.lgs. 24/2023 attuativo della Direttiva Whistleblowing*, in *Altalex*, 2023, 1;

BOUCHER, *How blockchain technology could change our lives*, in *European Parliamentary Research Service*, 2017, 1;

BRANTING, *An Issue-Oriented Approach to Judicial Document Assembly*, In *Proceedings of the Fourth International Conference on Artificial Intelligence and Law*, New York, 1993, 205;

BRICOLA, *Il costo del principio "societas delinquere non potest" nell'attuale dimensione del fenomeno societario*, in *Riv. It. Dir. Proc. Pen.*, 1970, 945;

BURCHARD, *Digital Criminal Compliance*, in Engelhart, Kudlich, Vogel (a cura di), *Digitalisierung, Globalisierung und Risikoprävention. Festschrift für Ulrich Sieber*, Berlino, 2021;

BURCHARD, *L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società*, in *RIDPP*, 2020, 22;

BURTIN, HOULE, *Investigazioni interne: uno sguardo all'esperienza americana*, in CENTONZE, MANTOVANI (a cura di), *La responsabilità "penale" degli enti. Dieci proposte di riforma*, Bologna, 2016;

CALIFANO, *Ecosistemi digitali, Trasformazioni sociali e rivoluzione tecnologica XXII edizione dei Colloqui internazionali di Cortona,* in *Fondazione Giacomo Fetrinelli*, Milano, 2019, 10;

CANZIO, *Il dubbio e la legge*, in *Diritto penale contemporaneo*, 2018, 1;

CAPACCIOLI, *DLT e Blockchain*, in Ziccardi, PERRI (a cura di), *Tecnologia e diritto*, Vol II, Milano, 2019;

CAPOBIANCO, *Privacy e controlli a distanza :ultimi approdi normativi e giurisprudenziali*, in *SalvisJuribus*, 2018, 5;

CAPPELLINI, *Machina delinquere non potest? brevi appunti su intelligenza artificiale e responsabilità penale*, in *Discrimen*, 2019, 10;

CARBONE, *Smart contracts: caratteristiche tecniche e tecnologiche*, in

BATTAGLINI, GIORDANO (a cura di), *Blockchain e Smart contracts*, Milano, 2019;

CASONATO, *Giustizia e intelligenza artificiale: considerazioni introduttive,* in *BioLaw Journal – Riv. di BioDiritto*, 2021, 350;

CASTELFRANCHI, *Six critical remarks on science and the construction of the knowledge society*, in *Journal of Science Communication*, 2007, 1;

CASTELLI, PIANA, *Giustizia predittiva. La qualità della giustizia in due tempi*, in *Questione Giustizia*, 2018, 153;

CATTANEO, *Le indagini interne: presupposti, finalità e aspetti operativi*, *Atti del* Convegno *AODV231 – "L'Organismo di Vigilanza tra Indagini Interne e Investigazioni Processuali"*, Milano, 2013;

COLACURCI, *L'idoneità del modello nel sistema 231, tra difficoltà operative e possibili correttivi*, in *Dir. Pen. Cont*., 2016, 60;

COLACURCI, L'illecito "riparato dell'ente", Torino, 2022;

COMOGLIO, *Prefazione*, in NIEVA, FENOLL, *Intelligenza artificiale e processo*, 2018, trad. it., Torino, 2019;

CORBELLA, POZZA, *"Modello 231" e "Sistema di controllo interno": aree di sovrepposizione e profili di differenziazione. Implicazioni in termini di costi e benefici sugli assetti degli organi di controllo e vigilanza, in* CENTONZE, MANTOVANI *(a cura di), La responsabilità "penale" degli enti Dieci proposte di riforma*, Bologna, 2016;

COSIMI, *Origine dei "Big Data"*, in *Gnosis*, 2017, 130;

COTTONE, MANTOVANI, *La reazione dell'impresa a fronte di «segnali di allarme» e/o di indagini della magistratura*, in BONELLI, MANTOVANI (a cura di), *Corruzione nazionale e internazionale*, Milano, 2014;

D'ACQUARONE, ROSCINI-VITALI, *L'investigazione interna nel procedimento a carico dell'ente: alcuni spunti per l'integrazione del modello di organizzazione di gestione,* in *La resp amm. soc. e enti*, 2020, 1;

D'AGOSTINO, *Criminal Compliance e nuove tecnologie*, in corso di pubblicazione, 1;

D'APONTE, *I controlli a distanza e la videosorveglianza nei luoghi di lavoro tra diritto nazionale e giurisprudenza CEDU*, in *Rivista giuridica del lavoro e della previdenza sociale*, 2020, 238;

DE ANGELIS, ZANFINO, ANIELLO, LOMBARDI, SASSONE, *Evaluating Blockchain Systems: A Comprehensive Study of Security and Dependability Attributes*, Roma, 2022;

DE MAGLIE, *L'etica e il mercato. La responsabilità penale delle società,* Milano, 2002;

DE SIMONE, *La responsabilità da reato degli enti nel sistema sanzionatorio italiano: alcuni aspetti problematici*, in *Riv. Trim. dir. Pen. econ*., 2004, 671;

DE SIMONE, *Profili di diritto comparato*, in LATTANZI, SEVERINO (a cura di), *Responsabilità da reato*, vol. I, Torino, 2021, 5 s.

DE VERO, *La responsabilità penale delle persone giuridiche*, Torino, 2008;

DI GIOVINE, *Lineamenti sostanziali del nuovo illecito punitivo*, in LATTANZI (a cura di), *Reati e responsabilità degli enti. Guida al d.lgs. 8 giugno 2001, n. 231*, Torino, 2010;

DI GIOVINE, *Il criterio di imputazione soggettiva*, in LATTANZI, SEVERINO (a cura di), *Responsabilità da reato degli enti*, vol I, diritto sostanziale, Torino, 2020;

DIAMANTIS, *The Problem of Algorithmic Corporate Misconduct*, in SSRN, 2019, 3;

DOMINGOS, *A Few Useful Things to Know about Machine Learning*, in *Communications of the* ACM, 2012, 75;

FALSONE, *L'infelice giurisprudenza in materia di controlli occulti e le prospettive del suo superamento*, in *Riv. It. Dir. Lav*., 2015, 984;

FERGUSON, *Big data and predictive reasonable suspicion*, in *University of Pennsylvania* law review, 2015, 351;

FERGUSON, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, New York, 2017;

FERRARESE, *Presentazione dell'edizione italiana di* GARAPON, LASSEGUE, *La giustizia digitale*, Bologna, 2021;

FIDELBO, *L'accertamento dell'idoneità del modello organizzativo in sede giudiziale*, in A.M STILE, MONGILLO, G. STILE (a cura di), *La responsabilità da reato degli enti collettivi: a dieci anni dal d.lgs. n. 231/2001*, Napoli, 2013, 170;

FORTUNATO, DI NOCCO, *Corporate Governance. Le fasi e i processi operativi di un'indagine interna o «internal investigation»*, in *Riv. dott. comm*., 2018, 234;

FUSCO, PALIERO, *L'"happy end" di una saga giudiziaria: La colpa di organizzazione trova "forse" il su tipo*, in *Sistema Penale*, 2022, 124;

GAMBINO, BOMPREZZI, *Blockchain e protezione dei dati* personali, in *Dir. Inf*, 2019, 624;

GARDNER, An Artificial Intelligence Approach to Legal Reasoning, Cambridge, 1987;

GHIANI, *Blockchain: linee guida*, 2022, Torino;

GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assesment tools tra Stati uniti ed Europa*, in *Dir. Pen. Cont*., 1;

GIANNINI, *Artificial Intelligence, human oversight and criminal liability: an european strenght test*, in *Criminalia*, 2021, 1;

GULLO, *I modelli organizzativi*, in Lattanzi, Severino (a cura di), *Responsabilità da reato degli enti*, vol. I, Torino, 2020;

GULLO, *I reati informatici*, in LATTANZI, SEVERINO (a cura di), *Responsabilità da reato*, vol. I, Torino, 2020;

GULLO, *Compliance*, in *Archivio Penale*, 2023, 1;

HALLEVY, *The Criminal Liability of Articial Intelligence Entities. From ScienceFiction to Legal Social Control*, in *Akron. Intell. Prop.J*., 2010, 170;

HARRY, SURDEN, *Artificial Intelligence and Law: An Overview*, vol. 35, *Ga. St. U. L. Rev*, 2019, 1330;

ITALIANO, *Intelligenza Artificiale: passato, presente, futuro*, in PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018;

JAIN, KULKARNI, SHAH, *Natural Language Processing*, in *International Journal of Computer Sciences and Engineering*, 2018, 1;

KAELBLING, LITTMAN, MOORE, *Reiforcment learning: a survey, in Journal of Artificial Intelligence*, 1996, 235;

LAGHI, TELITI, *Processo, processi e rivoluzione tecnologica*, Padova, 2022;

LAUFER, *Inautenticità del sistema della responsabilità degli enti e giudizio di colpevolezza*, in CENTONZE, MANTOVANI (a cura di), *La responsabilità "penale" degli enti. Dieci proposte di riforma*, Bologna, 2016;

LAVORGNA, SUFFIA, *La nuova proposta europea per regolamentare i Sistemi di Intelligenza Artificiale e la sua rilevanza nell'ambito della giustizia penale*, in *Riv. Trim.*, 2021, 89;

LO SAPIO, *La trasparenza sul banco di prova dei modelli algoritmici*, in *Federalismi.it*, 2021, 242;

LONGO, *Il test di turing storia e significato*, in *Mondo Digitale*, 2009, 1;

MAGLIE, *L'etica e il mercato. La responsabilità penale delle società*, Roma, 2002;

MANACORDA, *L'idoneita` preventiva dei modelli di organizzazione nella responsabilita`da reato degli enti: analisi critica e linee evolutive*, in *Riv. trim. dir. pen. econ*, 2017, 50;

MANCUSO, *Le investigazioni interne nel procedimento a carico dell'ente*, in CASTRONUOVO, DE SIMONE, GINEVRA, LIONZO, NEGRI, VARRASO (a cura di), *Compliance. Responsabilità da reato degli enti collettivi*, Milano, 2019;

MANCUSO, *Le investigazioni interne nel sistema processuale italiano: tra vuoto normativo e prassi applicative incerte*, in *Convegno Associazione dei componenti degli Organismo di Vigilanza – aodv231*, 2018, 1;

MANES, TRIPODI, *L'idoneità del modello organizzativo* in CENTONZE, MANTOVANI (a cura di), *La responsabilità "penale" degli enti. Dieci proposte di riforma*, Bologna, 2016;

MARTINELLI, *Il controllo a distanza del lavoratore e nuove tecnologie*, in *Ciberspazio e diritto*, 2015, 350;

MAZZACUVA, *La diversione processuali per gli enti collettivi nell'esperienza anglo-americana. Alcuni spunti* de iure condendo, in *Dir. Pen. Cont. – Riv. Trim.*, 2016, 80;

MCCARTHY, MINSKY, ROCHESTER, SHANNON, *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, in *AI Magazine*, 2006, 10;

MIK, *Smart Contracts: Terminology, Technical Limitations and Real-World Complexity*, in *SSRN*, 2017, 1;

MILANO, *Turning a light on our implicit biases,* in *Harvard Gazzette,* 2020, 1;

MINELLI, *La responsabilità "penale" tra persona fisica e corporation alla luce della Proposta di Regolamento sull'Intelligenza Artificiale*, in *Riv. Trim. Dir. Cont. Pen.*, 2/2022, 50;

MOHAMMED, KHAN, BASHIER, *Machine Learning, Algorithms and Applications*, Boca Raton, 2017;

MONGILLO, BELLACOSA, *Il sistema sanzionatorio*, in LATTANZI, SEVERINO (a cura di), *Responsabilità da reato degli enti*, vol. I, Torino, 2020;

MONGILLO, *Il giudizio di idoneità del Modello di organizzazione ex d.lgs. 231/2001: incertezza dei parametri di riferimento e prospettive di soluzione,* in *La resp. Amm. delle società e degli enti*, 2011, 1;

MONGILLO, *Presente e futuro della compliance penale*, in *Sist. pen*., 2022, 1;

MONTESANO, *Il caso Impregilo: la Cassazione definisce delle regole più rigorose in relazione all'accertamento della efficacia dei modelli organizzativi (Commento a Cass. pen., Sez. V, n. 4677, 30 gennaio 2014),* in *Rivista 231*, 100;

MORABITO, *La chiave del crimine*, in *Poliziamoderna*, 2015, 36;

MORGANTE, FIORINELLI, Promesse e rischi della compliance penale digitalizzata, in *Arch. Pen*, 2022; 1;

MOSCO, *Roboboard. L'intelligenza artificiale nei consigli di Amministrazione*, in *Analisi giuridica dell'economia*, 2019, 250;

NATALE, *La qualità dei dati e la ISO/IEC 25012*, in *U&C n.2*, 2019, 1;

NICOLICCHIA, *Corporate Internal Investigations e diritti dell'imputato del reato presupposto nell'ambito della responsabilità «penale» degli enti: alcuni rilievi sulla base della «lezione americana»*", in *Riv. Trim. Dir. Pen. Ec*., 2014, 775;

NIETO, *Internal Investigations, Whistle-Blowing, and Cooperation: The Struggle for Information in the Criminal Process*, in MANACORDA, CENTONZE, FORTI (eds.), *Preventing Corporate Corruption. The Anti-Bribery Compliance Mode*l, Londra, 2014;

NISCO*, Prospettive penalistiche del controllo a distanza sull'attività lavorativa nell'attuale contesto normativo e tecnologico, in Riv. Trim. Dir. Cont. Pen,* 2021, 90;

NISCO, *Riflessi della compliance digitale in ambito 231*, in *Sist. pen*., 2022, 1;

PALIERO, *La società punita: del come, del perché e del per cosa*, in *Riv. It. dir*., e *proc. pen*., 2008, 1540;

PALIERO, SALAFIA, *L'imputazione della responsabilità all'ente per il fatto-reato dei soggetti apicali: il punto di vista della Cassazione*, in *Le Soc.*, 2014, 469;

PALIERO, PIERGALLINI, *La colpa di organizzazione*, in *Resp. Amm. Soc. ed enti*, 2006, 170;

PALIERO, *Responsabilità dell'ente e cause di esclusione della colpevolezza: decisione «lassista» o interpretazione costituzionalmente orientata?*, commento a sentenza G.U.P. Trib. Milano (Manzi), 17 Novembre 2009, in *Le Società*, 2010, 477;

PALMIRANI, *Big Data e conoscenza*, in *Riv. filos. dir*., 2020, 70;

PANATTONI, *Ai and criminal law: the myth of 'control' in a data-driven society*, in Vermeulen, Persak, Recchia (a cura di), *Artificial Intelligence, Big Data and Automated Decision-Making* in *Criminal Justice*, in *RIDP*, 2021, 128;

PATERNOSTER, SIMPSON, *A Rationale Choice Theory in Corporate Crime*, in CLARKE, FELSON (a cura di), *Routine Activity and Rational Choice*, vol. 5, Londra, 1993;

PELISSERO, SCAROINA, NAPOLEONI, *Principi generali*, in LATTANZI, SEVERINO (a cura di), *Responsabilità da reato degli enti*, Torino, 2020;

PETHE, RIPPEY, KALE, *A Specialized Expert System for Judicial Decision Support*, *In Proceedings of the Second International Conference on Artificial Intelligence and Law*, New York, 1989;

PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in CADOPPI, CANESTRARI, MANNA, PAPA (a cura di), *Cybercrime*, 2019, Torino, 40;

PIERGALLINI, *I modelli organizzativi*, in AA. VV., LATTANZI (a cura di), *Reati e responsabilità degli enti. Guida al d.lgs. 8 giugno 2001, n. 231*, 2010;

PIERGALLINI, *Paradigmatica dell'autocontrollo penale: dalla funzione alla struttura del 'modello organizzativo' ex d. lgs. 231/2001*, in *Cass. pen*., 2013, 862

PIERGALLINI, *Intelligenza artificiale:da 'mezzo' ad 'autore' del reato*?, Torino, 2020;

PIERGALLINI, *Una sentenza "modello" della cassazione pone fine all'estenuante vicenda "Impregilo"*, in *Sistema penale*, 2022, 1;

PIZZETTI, *Il procedimento italiano di adeguamento al GDRP e la struttura del Codice novellato*, in PIZZETTI (a cura di), *Protezione dei dati personali in Italia tra GDPR e codice novellato*, Milano, 2022;

PIZZETTI, *Il sistema normativo di protezione dei trattamenti di dati personali nel quadro europeo e nazionale*, in PIZZETTI (a cura di), *Protezione dei dati personali in Italia tra GDPR e Codice Privacy*, Milano, 2022;

PULITANÒ, *La responsabilità "da reato" degli enti: i criteri di imputazione*, in *Riv. It. dir.proc. pen*., 2002, 405;

QUATTROCOLO, *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente discussione tra scienze penali e informatiche*, in *Leg. pen*., 2018, 1;

QUATTROCOLO, *Qualcosa di meglio del diritto (e del processo) penale?*, in *disCRIMEN*, 2020, 1;

QUEST, CHARRIE, CROO DE JONGH, ROY, *The risks and benefits of using AI to detect a crime*, in *Harvard Business review*, 2018, 5;

RIAHi, *Big Data and Big Data Analytics: Concepts, Types and Technologies*, in *IJRE*, 2018, 350;

ROMANO, *Diritto, robotica e teoria dei giochi: riflessioni su una sinergia*, in ALPA (a cura di), *Diritto e intelligenza artificiale*, Pisa, 2020;.

RUGGIERO, *Scelte discrezionali del pubblico ministero e ruolo dei modelli organizzativi nell'azione contro gli enti*, Torino, 2018;

RUSSEL, NORVIG, *Artificial Intelligence – A modern approach*, ed. III, Londra, 2010;

RUSSO, *I modelli di organizzazione, gestione e controllo. Letteratura, prassi e innovazioni tecnologiche*, Milano, 2022;

SABIA, *Artificial intelligence and environmental criminal Compliance*, in ESPINOZA DE LOS MONTEROS DE LA PARRA, GULLO, MAZZACUVA (a cura di), *The Criminal Law Protection of our Common Home*, Roma, 2019;

SABIA, *Responsabilità da reato degli enti e paradigmi di validazione dei modelli organizzativi*, Torino, 2022;

SALANITRO, *Intelligenza artificiale e responsabilità: la strategia della commissione europea*, in *Riv. Dir. Civ*., 2020, 1245;

SALVADORI, *Agenti artificiali, opacità, tecnologica e distribuzione della responsabilità penale*, in *Riv. It. Dir. Proc. Pen.*, 2021, 60;

SARKER, *Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions*, in *SN Computer Science*, 2021, 1;

SARTOR, BRANTING, *Introduction: judicial applications of artificial intelligence*, in *Artificial intelligence and law*, 1998;

SCHEMMEL-DIETZEN, *"Effective Corporate Governance" by Legal Tech & Digital Compliance*, in BREIDENBACH, GLATZ, *Rechtshandbuch Legal Tech*, Monaco di Baviera, 2018;

SEARLE, *Minds, Brains and Programmes*, Londra, 1980;

SELVAGGI, *L'interesse dell'ente collettivo quale criterio di ascrizione della responsabilità da reato*, Napoli, 2006;

SEVERINO, *Il sistema di responsabilità degli enti ex d.lgs. n. 231/2001: alcuni problemi aperti*, in CENTONZE, MANTOVANI (eds.), *La responsabilità «penale» degli enti. Dieci proposte di riforma*, Bologna, 2016;

SEVERINO, *Intelligenza artificiale e diritto penale*, in RUFFOLO (a cura di), *Intelligenza artificiale: il diritto, i diritti, l'etica*, 2020;

SIMBULA, *Normativa italiana sulle DLT*, in BATTAGLINI, GIORDANO (a cura di), *Blockchain e Smart contracts*, Milano, 2019;

SIMONCINI, SUWEIS, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Rivista di filosofia del diritto*, 2019, 95;

SASSI, *Gli algoritmi nelle decisioni pubbliche tra trasparenza e responsabilità*, in *Analisi Giuridica dell'Economia*, 2019, 100;

SPILLER, *Il diritto di comprendere, il dovere di spiegare. "Explainability" e intelligenza artificiale costituzionalmente orientata (The right to understand, the duty to explain. Explainability and constitutional oriented artificial intelligence)*, in *BioLaw Journal - Rivista di BioDiritto*, 2021, 410;

STROZZI, MASTROIANNI, *Diritto dell'unione europea parte istituzionale*, Roma, 2020;

TOMBARI, *Governo Societario, compliance e "indagini interne" nella s.p.a. quotata*, in ROSSI (a cura di), *La corporate compliance: una nuova frontiera per il diritto*, Milano, 2017;

TONINI, CONTI, *Manuale di procedura penale*, Milano, 2021;

TREZZA, *L'Intelligenza Artificiale come ausilio alla standardizzazione del modello 231: vantaggi "possibili" e rischi "celati",* in *Giurisprudenza Penale Web*, 2021, 1;

TRIPODI, *Uomo, societas, machina*, in *Legislazione penale*, 2023;

TURING, *Computing Machinery and Intelligence*, in *Mind*, 1950;

UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano* significativo, in *Riv. Dir. pen. cont*., 2020, 77;

UÇAR, NOUR, SINDI, POLAT, *The Effect of Training and Testing Process on Machine Learning in Biomedical Datasets*, in *Hindawi, Mathematical Problems in Engineering*, 2020, 1;

VARRASO, *Il procedimento per gli illeciti amministrativi dipendenti da reato*, Milano, 2012;

VERMEULEN, PERŠAK, RECCHIA, *Artificial Intelligence, Big Data and Automated Decision-Making in Criminal Justice*, in *RIDP*, 2021, 110;

VIANELLI, VALENTI, *RegTech e Modelli 231: uno sguardo al futuro per un'esigenza presente*, in *Giurisprudenza Penale*, 2021, 1;

VIGLIANISI, *Le nuove frontiere dell'intelligenza artificiale ed i potenziali. Rischi per il diritto alla "privacy"*, in *Persona e Mercato*, 2021, 390;

WEIZENBAUM, *Computer Power and Human Reason*, San Francisco, 1976;

WITTEN, FRANK, HALL, *Data mining. Practical Machin Learning Tools and Techniques*, Burligton, 2011;

WRIGHT, DE FILIPPI, *Decentralized Blockchain Technology and The Rise of Lex Cryptographia*, in *Social Science Research Network*, 2015, 1;

YATES, *Paura e società del rischio. Un'intervista a Urlich Beck*, in *Lo Sguardo*, 2016, II, 213;

ZAKIR, SEYMOUR, BERG, *Big data analytics*, in *Issues in Information Systems*, vol. XVI, 2015, 80;

ZUDDAS, *Brevi note sulla trasparenza algoritmica*, in *Amministrazione in cammino*, 2020, 10.