INTELLIGENZA ARTIFICIALE E MOG 231: DALLA COLPA D'ORGANIZZAZIONE ALLA COLPA "ARTIFICIALE"

Giuseppe Imbrigiotta

Sommario: 1. Nozioni introduttive sull'Artificial Intelligence; 2. L'esigenza di una regolamentazione di settore: l'impulso sovrannazionale; 3. Brevi cenni sulla colpa di organizzazione; 3.1 ...e sul modello di organizzazione e gestione di cui al D.Lgs. 231/2001; 4. "*Risk assestment tools*" e redazione del modello di gestione, organizzazione e controllo nell'era della compliance digitale; 5. Risvolti sulla responsabilità dell'ente per colpa organizzativa.

ABSTRACT

Il presente contributo, ha lo scopo di porre l'attenzione sui possibili effetti che dall'innovazione tecnologica in materia di intelligenza artificiale possano derivare nel settore giuridico. Dopo una breve ricognizione e descrizione delle principali fonti giuridiche che regolano la programmazione, commercializzazione e le modalità d'impiego di tali strumenti di intelligenza artificiale, si è cercato di comprendere le conseguenze dell'utilizzo di software *AI* nel settore della *compliance* aziendale. E' stata esposta, dunque, la disciplina in tema di "colpa d'organizzazione" dell'ente e la concreta applicazione che la giurisprudenza fa delle norme di cui agli artt. 6 e 7 del D.Lgs. 231/01. Infine, ci si è posti il problema di comprendere quali potessero essere le conseguenze in tema di responsabilità da colpa di organizzazione dell'ente che abbia affidato la gestione del proprio modello organizzativo e di gestione ad un *software AI*, evidenziando, inoltre, l'esigenza di un adeguamento della normativa di settore e, forse, ad un ripensamento della struttura della colpa d'organizzazione.

The present elaborate aims at pointing out the possible risks related to the technological advance in artificial intelligence (hereafter "AI") in the juridical sector. After a brief overview on the principal legal sources regulating the programming, commercialisation and means of employment of AI instruments, it will try to comprehend the consequences of AI in company compliance. Hence, in light of the concept of "organisarional fault" and the actual judicial interpretation of articles 6 and 7 of the DLgs 231/01, the author tackled the possible consequences in case of company responsibility following the adoption of an AI generated or implemented internal compliance model suggesting a rethinking of the actual norm in matter of organisational fault.

Nozioni introduttive sull'*Artificial Intelligence*

La "rivoluzione *cybernetica*", tramite la creazione di *software* di intelligenza artificiale, è ormai in corso da anni

e sta pian piano cambiando il modo di concepire le attività umane, persino quelle che un tempo erano ritenute insostituibili.

Se all'origine poteva essere sostenuto che lo sfruttamento di questa tecnologia si arrestasse a quei settori fondati su schemi prestabiliti, in cui vi è una grande quantità di dati da processare nel più breve tempo possibile, individuando la correlazione statistica mediante la programmazione di algoritmi specifici[1], oggi l'*AI* potrebbe essere utilizzata anche in settori differenti e più complessi come quello giuridico, della sicurezza pubblica, medico, automobilistico etc[2].

In particolare, nel rapporto tra questa "rivoluzione" ed il settore giuridico alcuni autori[3] hanno prospettato una ripartizione dei settori in cui l'*AI* produrrebbe effetti che potrebbero riverberarsi sui principi e le libertà fondamentali dell'uomo.

In particolare: a) in ottica predittiva e preventiva potrebbe essere impiegata come supporto alle attività di *predict policing**[4]***, quali pattugliamenti, identificazioni ed interventi preventivi; b) in ottica decisionale, i cd. *automated decision systems*, potrebbero essere utilizzati algoritmi in grado di addivenire ad una statuizione in ordine a contenziosi civili, amministrativi e, forse con maggiori problemi, anche penali; c) sempre per la sua funzione predittiva, potrebbe essere impiegata per la valutazione della pericolosità criminale degli individui al fine di semplificare le indagini; d) l'accertamento della responsabilità quando l'*AI* sia stato lo strumento per commettere un illecito o, comunque, quando l'attività del *software* abbia concorso alla commissione del delitto.

Se le ipotesi in cui tale tecnologia è uno strumento di supporto all'attività umana non pongono particolari problemi, permanendo in capo all'uomo la decisione definitiva, i punti b), c) e d) creano importanti problemi dogmatici ed etici.

In primo luogo, escludendo aprioristicamente che *machina delinquere potest**[5]***, il tema verterebbe sull'individuazione del soggetto che si trovi in una posizione di dominio o, comunque, rivesta una posizione di garanzia e, dunque, sul soggetto che abbia il dovere di impedire che la macchina commetta il reato; le principali soluzioni riguardano la posizione del proprietario del bene, del programmatore, del venditore ed il problematico rapporto con la responsabilità da prodotto difettoso[6].

Quanto al punto b), invece, l'attività decisionale di ogni contenzioso giudiziario reca inevitabilmente una

componente materiale, attinente al rigore legislativo ed alla tassatività delle norme, ma è innegabile che nella decisione finale permane un'ineliminabile componente soggettiva e morale legata alla concezione ed interpretazione delle norme mediante una loro lettura "eticamente" influenzata.

Conseguentemente, tutte le decisioni saranno private di questo "errore umano" e si sostanzieranno in un'applicazione adiafora del diritto, posto che per il modo in cui l'intelligenza artificiale è programmata «fallirà proprio i compiti che richiedono un apprezzamento in chiave assiologica»[7].

Inoltre, con particolare riferimento alle decisioni nel campo del diritto penale, poiché la prova testimoniale è spesso il fulcro del processo, permangono dubbi sulla capacità dell'*AI* di valutare l'attendibilità di un teste nonché la sua capacità di esprimere un giudizio circa la gravità, concordanza e precisione degli indizi ai sensi dell'art. 192, co. 2, c.p.p.[8]

Tali rischi non sono di poco conto alla luce delle considerazioni che seguiranno.

Infatti, ulteriore questione, da non sottovalutare, attiene alla distinzione tra intelligenza artificiale dotata di *Machine Learning* ed *AI* che ne sono prive.

In effetti, se l'attività ermeneutica è già di per sé complessa, la programmazione di un *judge-bot**[9]* condurrebbe all'annichilimento dell'attività interpretativa, sostanziandosi in un'impossibilità di letture divergenti da quelle imposte dall'algoritmo, e, di contro, ad un'assoluta certezza del diritto. Letture che risentono, necessariamente, della gerarchia di valori stabilita dal programmatore[10].

In tal modo si rischia di inibire la funzione di garanzia del sistema dei tre gradi di giudizio, d'altronde, trattandosi di una programmazione prestabilita, vi sarebbe il pericolo che il *software,* ripercorrendo la vicenda con le stesse lenti in ogni grado di giudizio, giungerebbe sempre alla medesima conclusione.

Diversamente, nell'ipotesi di *AI* dotata di *Maching Learning*[11], ovverosia quella particolare tipologia di programmazione che permette al *software* di acquisire dati dalla propria esperienza al fine di elaborare nuove strategie per affrontare problemi futuri, potrebbe aversi un'instabilità dell'interpretazione normativa, con la conseguente impossibilità di prevedere gli esiti dell'attività ermeneutica della macchina.

L'importanza della regolamentazione dell'utilizzo dell'intelligenza artificiale si manifesta anche per quelle attività di sussidio all'uomo che si sostanziano nell'organizzazione e nell'analisi statistica di dati. Un esempio potrebbe essere la creazione di algoritmi in grado di raccogliere norme giuridiche ed informazioni aziendali, per valutare il *risk assestment* e predisporre le misure più idonee a prevenire la commissione di reati o la verificazione di eventi il cui rischio è stato valutato[12].

Il tema è attuale e richiede un'analisi delle fonti normative che regolano il settore della programmazione, utilizzazione e commercializzazione di *software* di intelligenza artificiale.

1. **L'esigenza di una regolamentazione di settore: l'impulso sovrannazionale**

I primi atti di *softlaw*, in questo innovativo settore, sono stati promossi da organizzazioni internazionali che hanno fissato i principi e linee guida rivolti a legislatori nazionali ed internazionali, al fine di predisporre una normativa minima che regoli i doveri e poteri dei produttori, programmatori ed utilizzatori delle tecnologie di *AI**[13]*.

Tra queste fonti può essere citata la cd. Dichiarazione di *Asilomar*, frutto del contraddittorio di esperti *AI* e giuristi che si sono confrontati sul tema nella *Asilomar Conference on Beneficial* del 2017. Tale dichiarazione, suddivisa in tre settori - ricerca, etica e valori, problemi a lungo termine - cristallizza i principi che dovrebbero essere seguiti nell'utilizzo e nella programmazione di queste tecnologie[14].

Ulteriore passo in avanti è stato fatto grazie alla Commissione europea per l'efficacia della giustizia (CEPEJ)[15], organismo istituito dal Comitato dei Ministri del Consiglio d'Europa, che ha stilato la "*Carta etica europea per l'uso dell'intelligenza artificiale nei sistemi di giustizia penale e nei relativi ambienti*"[16]. Tale Carta, adottata il 4 dicembre 2018, è rivolta a soggetti pubblici e privati e stabilisce i principi[17] che i Legislatori dovrebbero seguire nell'elaborazione della normativa sullo sviluppo, la verifica e l'utilizzo di questi sistemi.

Il principale scopo è, dunque, quello di ispirare gli Stati e le Organizzazioni internazionali a potenziare i sistemi giudiziari mediante l'utilizzo di questi *software*, nel rispetto della sicurezza e delle garanzie dei cittadini.[18]

Sebbene si tratti di un atto di *softlaw*, dunque, sprovvisto di efficacia vincolante, la sua analisi comparativa e

la valutazione dei benefici e dei rischi unita alla predisposizione dei principi per un corretto e "giusto" utilizzo di *tools AI* hanno consentito a tale atto di avere una diffusione globale.

Un chiaro esempio di tale diffusività è proprio l'emanazione del "*Blueprint for an AI Bill of rights*"[19] statunitense, del 2022; si tratta del progetto di una carta dei diritti sull'intelligenza artificiale al cui interno sono sanciti i principi che dovranno essere rispettati nello sviluppo ed utilizzo della stessa, con un'evidente ispirazione alla Carta etica europea.

Con riguardo, invece, all'Eurozona, il Consiglio d'Europa ha adottato la "*Convenzione quadro sull'Intelligenza Artificiale e i diritti umani, la democrazia e lo stato di diritto*"[20], del 17 maggio 2024, affinché via sia una maggiore armonizzazione e, soprattutto, il rispetto dei principi suddetti, tra le normative che gli Stati membri adotteranno.

Infine, il primo atto legislativo al mondo che ha disposto una disciplina di settore vincolante è di matrice europea.

L'Unione Europea ha, infatti, approvato l'*Artificial Intelligence Act (AI Act)****[21]***, ossia il regolamento (UE) 2024/1689 del 13 giugno 2024, con il dichiarato scopo di consentire lo sviluppo, la commercializzazione e l'utilizzo di strumenti di intelligenza artificiale all'interno dell'Unione Europea, nel rispetto della sicurezza e dei diritti fondamentali dell'uomo.

L'art. 5 del Regolamento, rubricato "pratiche di *AI* vietate", pone il divieto di immissione, messa in servizio ed utilizzo di alcune funzioni o modalità d'uso di questi sistemi poiché ritenute potenzialmente lesive della sicurezza e dei diritti fondamentali.

In particolare, è vietato l'utilizzo o la messa in commercio di sistemi di intelligenza artificiale che sfruttino tecniche subliminali o volutamente decettive, al fine di indurre una persona od un gruppo di persone a prendere una decisione che altrimenti non avrebbe preso.

La funzione è quella di tutelare il consenso informato di ogni individuo, pertanto, in tutti quei casi in cui l'informazione è obbligatoria (prestazioni sanitarie; contratti bancari; etc..), non potranno essere utilizzati sistemi di intelligenza artificiale in modo fraudolento per indurre in errore i destinatari dell'informazione ad effettuare una scelta.

Il divieto si estende anche a quei *software* che abbiano lo scopo di valutare o classificare persone fisiche o gruppi di persone in base al loro comportamento, caratteristiche o personalità, se da tale valutazione possa derivare un trattamento pregiudizievole sproporzionato rispetto al comportamento analizzato o, comunque, un trattamento sfavorevole in contesti sconnessi da quelli in cui i dati sono stati raccolti.

Ulteriore proibizione riguarda l'immissione nel mercato o l'utilizzo di *tools AI* capaci di prevedere se un individuo possa commettere dei reati, fondando tale valutazione sulle caratteristiche o sui tratti personali del soggetto esaminato.

La norma, tuttavia, prevede una deroga quando l'utilizzo dello strumento *AI* sia volto "*a sostegno della valutazione umana del coinvolgimento di una persona in un'attività criminosa, che si basa già su fatti oggettivi e verificabili*". Tale funzione predittiva, basata su schemi presuntivi, rischia di danneggiare i soggetti sottoposti a tale valutazione, sostanziandosi in un giudizio "lombrosiano" di pericolosità sociale.

Infine, con riguardo a quei sistemi di identificazione biometrica remota "in tempo reale" utilizzabili in luoghi pubblici per le attività di contrasto alla criminalità, pone il medesimo divieto salvo che questo non sia essenziale:

- per la ricerca mirata di vittime di sfruttamento sessuale o tratta di esseri umani nonché per la ricerca di persone scomparse;
- per la prevenzione di minacce specifiche imminenti che pongono in pericolo la vita o l'incolumità pubblica;
- per la localizzazione ed identificazione, durante le indagini o per l'esecuzione di una sanzione penale, di un individuo sospettato di aver commesso un reato per cui la pena alla reclusione sia nel massimo di almeno quattro anni.

Nel predisporre tali divieti il Legislatore è stato particolarmente cauto.

Esso, ispirandosi ad un criterio di precauzione moderato, ha delineato il perimetro del rischio consentito, ritenendo prevalente l'interesse all'utilizzo dell'*AI* rispetto ai marginali rischi sui diritti che possano

concretizzarsi.

Invero, un tale bilanciamento d'interessi manifesta la convinzione delle istituzioni sovrannazionali circa i benefici che l'umanità potrà trarre da queste tecnologie[22].

D'altra parte, un approccio eccessivamente orientato alla precauzione, tale da rinunciare al miglioramento ed alla continua ricerca, avrebbe certamente impedito lo sviluppo di questa nuova tecnologia[23],

Possiamo, dunque, affermare che la legislazione europea, ha espresso la tollerabilità del rischio sociale legato all'utilizzo dell'*AI**[24]*, disponendo una regolamentazione equilibrata al fine di garantire, da un lato, il miglior sfruttamento dell'intelligenza artificiale, anche nel settore della giustizia predittiva e, dall'altro lato, quello di ridurre al minimo i rischi legati dal loro utilizzo.

Fatta questa premessa, appare verosimile che le società implementino applicazioni *AI*, nel rispetto della *ratio* del Regolamento europeo, per semplificare obblighi ed oneri dei vertici delle società sul "*risk assestment*" e sulla messa a punto di una *compliance* adeguata.

- **Brevi cenni sulla colpa di organizzazione**

Prima di entrare nel vivo dell'analisi della "*compliance digitale*", nell'accezione dottrinaria di questo termine[25], è opportuno descrivere brevemente il contenuto del D.Lgs 231/2001 con specifico riguardo all'onere per le società di dotarsi di un modello organizzativo.

Com'è noto, il legislatore ha predisposto due criteri d'imputazione.

Il primo è il criterio di imputazione oggettivo, previsto dall'art. 5 del D.Lgs. 231/2001, secondo cui l'ente risponde dell'illecito amministrativo in rilievo soltanto se il reato presupposto è stato commesso nel suo interesse od a suo vantaggio.

Il secondo, invece, è il criterio d'imputazione soggettivo, stabilito dall'art. 6 per i reati commessi da soggetti che rivestono posizioni apicali e dall'art. 7 per reati commessi dai sottoposti.

In virtù del criterio soggettivo, nel caso in cui soggetti attivi del reato presupposto siano dirigenti[26], l'ente non risponde dell'illecito amministrativo se venga fornita la prova:

- dell'adozione di un modello organizzativo e di gestione idoneo a prevenire la commissione di reati della stessa specie;
- dell'istituzione di un organismo di vigilanza indipendente con autonomi poteri di iniziativa e controllo;
- del fatto che non vi è stato un omesso controllo o un'insufficiente vigilanza dell'organismo di vigilanza;
- dell'elusione fraudolenta del modello di organizzazione e gestione da parte degli apicali, autori del reato presupposto.

Quanto all'ambiguità della disposizione di cui all'art. 6 del D.Lgs. 231/01, "*l'ente non risponde del reato se prova*", è pacifico, in dottrina e giurisprudenza, che l'onere di dimostrare la mancata adozione o l'inadeguatezza del modello organizzativo ricada sulla procura, d'altronde, diversamente argomentando si finirebbe con l'ammettere una presunzione di colpevolezza della persona giuridica[27].

Inoltre, per scongiurare l'affermazione di una responsabilità oggettiva dell'ente per fatto altrui, la giurisprudenza ha riconosciuto che il criterio oggettivo debba essere accompagnato dalla c.d. "colpa di organizzazione[28]" - di cui agli artt. 6 e 7 del D.Lgs 231/01 - intesa quale «*deficit dell'organizzazione o dell'attività, rispetto ad un modello di diligenza esigibile dalla persona giuridica nel suo insieme*»[29].

Ed appunto, posto che non vi è alcun'inversione dell'onere probatorio[30], l'accusa dovrà dimostrare la negligenza organizzativa sotto ogni aspetto, mentre i Giudici valuteranno la rimproverabilità dell'ente secondo i canoni tipici della responsabilità colposa[31].

Si può affermare, dunque, che la responsabilità per gli illeciti amministrativi dipendenti da reato è autonoma[32] rispetto a quella della persona fisica ed ha una struttura tale per cui il reato presupposto costituisce l'evento mentre l'auto-organizzazione della persona giuridica (*compliance* aziendale) è la condotta.

Pertanto, verificata l'adozione ed attuazione di un modello organizzativo sarà necessario accertare la sua

idoneità ad impedire la commissione di reati della stessa specie di quello commesso.

Tale accertamento della colpevolezza dovrà essere effettuato mediante un giudizio di prognosi postuma.

Il Giudice dovrà idealmente porsi nel momento in cui è stato commesso l'illecito e verificare se l'adozione ed attuazione del "modello virtuoso" avrebbero impedito o ridotto la possibilità di commettere reati della stessa specie.

In altre parole, occorre anche che l'evento-reato sia concretizzazione del rischio che la regola cautelare contenuta nel modello mirava ad evitare o minimizzare, per poi trarne le conclusioni in tema di colpevolezza dell'ente.

Chiaramente, la valutazione del rischio di commissione di specifici reati, le procedure volte ad evitare che essi vengano commessi, la predisposizione di poteri all'organismo di vigilanza, la predisposizione di un modello disciplinare per coloro che violino le procedure, sono tutti elementi che fondano la *compliance* e sono cristallizzati all'interno del modello organizzativo e di gestione[33].

Ne consegue che l'efficace adozione di tali modelli «*consente all'ente di non rispondere dell'illecito, ma la cui mancanza, di per sé, non può implicare un automatico addebito di responsabilità*»[34].

L'esclusione di responsabilità vi sarà purché non sia stata accertata una "colpa organizzativa", nel modello sia stato valutato il rischio di commissione dei reati della stessa specie di quello compiuto e siano state predisposte valide misure volte ad evitare o minimizzare il rischio della sua realizzazione.

- **… e sul modello di organizzazione e gestione di cui al D.Lgs. 231/2001**

Acquisito che il modello organizzativo ed il suo apparato ispettivo, ossia l'organismo di vigilanza, costituiscono un aspetto di fondamentale importanza nella valutazione dell'imputazione soggettiva, occorre soffermarsi sulle principali caratteristiche di questi due elementi.

In effetti, il Legislatore, ritenendo la prevenzione[35] il miglior strumento per ridurre i rischi di commissione

di reati, ha predisposto una disciplina che persegue l'obiettivo di indurre le persone giuridiche ad implementare la propria *compliance* penale[36], predisponendo regole di comportamento, procedure e sanzioni.

Si tratta, invero, di una strategia ispirata ai *compliance programs* statunitensi[37], che, proprio come i modelli organizzativi e di gestione previsti dal nostro ordinamento, sono dei modelli di comportamento finalizzati ad impedire reati o, comunque, a farne emergere la loro commissione.

Affinché venga riconosciuto l'effetto premiale derivante dall'adozione del modello organizzativo, consistente nell'esenzione della responsabilità da reato o - nel caso in cui il modello sia adottato dopo la commissione dell'illecito[38] - nell'attenuazione delle conseguenze sanzionatorie, il modello stesso deve possedere delle caratteristiche specifiche.

Gli artt. 6 e 7 del D.Lgs. 231/2001 tratteggiano, in chiave generale ed astratta, i caratteri che i modelli devono possedere per rispondere all'esigenza di:

- individuare le principali aree di rischio di commissione di reati;
- prevedere specifici protocolli per programmare la formazione ed attuazione delle decisioni in relazione ai reati da prevenire;
- individuare le modalità di gestione delle risorse economiche;
- prevedere obblighi di informazione periodici nei confronti dell'organismo di vigilanza;
- introdurre un sistema disciplinare volto a sanzionare la violazione delle procedure contenute nel modello.

L'art. 7, inoltre, fornisce una definizione specifica di efficace attuazione, stabilendo che nel modello devono essere previste delle procedure che consentano, periodicamente, l'agevole verifica della sua stessa attualità nonché le modalità per permettere la modifica sistematica delle procedure e di ogni inadeguatezza sopravvenuta.

D'altronde, come affermato da autorevole dottrina: «*una lettura della disciplina rispettosa del testo dovrebbe indirizzare a dimostrare che sono state predisposte efficaci barriere gestionali, procedurali ed ispettive contro condotte che incrementino oltre la misura consentita il rischio di reati; e che tali strumenti di difesa sono stati elusi con azioni altamente ingannevoli****[39]***».

Tuttavia, la disciplina dettata dal D.Lgs 231/2001, con riguardo agli aspetti strumentali, contenutistici ed istituzionali del modello, è eccessivamente generica poiché non pone alcun criterio oggettivo che possa orientare il Giudice circa l'idoneità del modello e la sua colpa d'organizzazione.

In conseguenza di tale *deficit* normativodi legalità e tassatività, il giudizio sul comportamento dell'ente e la valutazione dell'idoneità od inidoneità del modello è demandato all'esclusiva discrezionalità del giudicante[40].

Alla luce di quanto detto, il modello deve essere pensato e strutturato appositamente per la società che lo adotterà, in considerazione di tutte le peculiarità dell'organizzazione aziendale, del *core business* e delle principali aree di rischio; si può affermare che il modello 231 è una veste su misura che deve essere costantemente adattata ai cambiamenti dell'ente.

Ed appunto, per garantire la tempestiva riorganizzazione delle procedure e delle sanzioni in caso di violazione del modello, è necessario che lo stesso sia attuale e dinamico[41] e, dunque, in grado di conformarsi al costante ampliamento del catalogo dei reati presupposto ed ai nuovi e diversi rischi che, con il passare del tempo, sono in continua evoluzione.

Pertanto, "*L'adozione del compliance program rappresenta, secondo gli aziendalisti, «un fatto invasivo nel sistema d'impresa» tale da richiedere un «approccio progettuale di vasto respiro, assimilabile all'impegno dedicato in sede di pianificazione strategica»****[42]***".

Tale necessaria pianificazione prevede delle tappe propedeutiche, affinché si possa ambire ad un modello adatto alla società per il quale è redatto, che sono:

- un'analisi generale della società al fine di pervenire ad una conoscenza totalizzante, per individuare gli aspetti che, nelle fasi successive, saranno oggetto di puntuale approfondimento;

- una mappatura delle aree di rischio, ossia di quelle funzioni che, per il tipo di attività svolta, sono maggiormente suscettibili di commettere determinati reati;

- sulla base degli specifici rischi-reato individuati in ogni area, predisporre un sistema di controllo e dei protocolli idonei a prevenire ed impedire la commissione degli illeciti;

Nella prassi applicativa il modello è composto da una parte generale da una parte speciale.

Nella prima sono indicati i sistemi di *governance* dell'ente e tutte quelle informazioni che consentono di comprenderne la struttura societaria, l'istituzione e la composizione dell'organismo di vigilanza ed i suoi poteri e doveri, le modalità di individuazione delle violazioni ed il sistema disciplinare nonché il codice etico; diversamente, la seconda è composta dalla descrizione della struttura dei reati presupposto, previsti dal D.Lgs.231/2001, dall'identificazione delle aree di rischio con la valutazione del grado di pericolo di verificazione, il rinvio ai protocolli di cui alla parte speciale e i principi generali di condotta[43].

Solo all'esito di questa pianificazione e redazione il modello potrà essere adatto alla società ed approvato dal Consiglio di amministrazione.

Quanto all'Organismo di vigilanza[44], di cui all'art. 6 del D.Lgs. 231/2001, è nominato dall'organo gestionale della società che può optare per un organismo monocratico o collegiale, con l'unica condizione che sia garantita l'imparzialità e la terzietà.

Quanto ai suoi compiti, esso vigila sull'adeguatezza del modello, proponendo i doverosi aggiornamenti quando lo stesso non sia più attuale, ed è beneficiario dei così detti flussi informativi, ossia di quelle comunicazioni che gli organi dirigenziali devono trasmettere all'organismo affinché quest'ultimo verifichi il rispetto del modello stesso.

Inoltre, è dotato di poteri ispettivi e di controllo che evidenziano l'esistenza di un obbligo di sorveglianza, tuttavia, non sorretto da veri e propri poteri impeditivi.

In conclusione, il sistema così delineato evidenzia il geocentrismo del modello organizzativo e del suo "garante", ossia l'Organismo di vigilanza, che rappresentano degli indici fondamentali di congruità dell'intera

capacità organizzativa dell'ente per far fronte e per prevenire la commissione di reati da parte di soggetti legati all'ente stesso da un rapporto di rappresentazione organica.

- **"*Risk assestment tools*" e redazione del modello di gestione, organizzazione e controllo nell'era della *compliance* digitale**

Le considerazioni su esposte evidenziano le difficoltà di mantenere una *compliance* non solo adeguata ma soprattutto attuale, stante le continue mutazioni dovute ad agenti, spesso, estrinseci rispetto alla società.

La redazione del modello implica una conoscenza effettiva dell'ente e del suo organigramma, del suo oggetto sociale, delle varie funzioni e della struttura degli organi dirigenziali; ed è sulla base di tali informazioni che deve essere formulata una puntuale mappatura dei rischi di commissione di reati, che si sostanzia in una valutazione statistico/probabilistica tramite l'elaborazione dei dati anzidetti.

In base a tali circostanze ed all'evoluzione *cybernetica*, non deve stupire che alcune società hanno già iniziato a sperimentare *software* capaci di progettare e redigere autonomamente i modelli organizzativi e di gestione[45].

Il *focus* del problema riguarda i benefici ed i rischi della "*digital criminal compliance*[46]" e, soprattutto, i risvolti che dall'utilizzo di tali strumenti possano derivare sull'accertamento della responsabilità amministrativa dell'ente dipendente da reato.

In primo luogo, sebbene la programmazione del *software* sia essenziale, alla luce della distinzione già affrontata tra *AI* dotate di *maching learning* ed *AI* che ne sonosprovviste, è certo che la funzione innovativa di questi sistemi è quella di individuare tempestivamente le carenze organizzative dell'ente, sulla base dei rischi rilevati, al fine di dotare la persona giuridica di strumenti prevenzionistici attuali ed efficaci[47].

È, infatti, un dato ormai pacifico che l'intelligenza artificiale sia un validissimo strumento da integrare nella *compliance*, per ridurre al minimo l'alea d'impresa e consigliare al meglio gli amministratori nella gestione dell'impresa, sia quale strumento utilizzato dagli organi preposti alla vigilanza per consentire un intervento immediato.

Ma potrà essere utilizzata quale strumento per predisporre e migliorare la *compliance*? E, soprattutto, quali risvolti potrebbero conseguire in tema di colpevolezza dell'ente in caso di inidoneità di un modello predisposto dall'intelligenza artificiale?

Richiamando quanto detto nel primo paragrafo, i *software* di intelligenza artificiale avrebbero la possibilità di apprendere strategie efficaci, già adottate da altre macchine in situazioni analoghe, grazie ad un *cloud* comune, modificandole ed adattandole al caso concreto senza la necessità di un nuovo intervento del programmatore grazie al cd. *black box algorithms**[48]*.

Ad ogni modo, il pericolo insito nell'utilizzo dei *software* di valutazione del rischio, che si fondano esclusivamente sulla programmazione prestabilita dal creatore, è quello che il sistema risponda predisponendo misure analoghe in contesti societari simili ma non identici, lasciando, dunque, delle aree vulnerabili ai rischi di commissione di reati.

Viceversa, l'imprevedibilità dell'auto-apprendimento, cd. *machine learning*, impedirebbe all'ente di governare e, dunque, indirizzare il *software* su determinati aspetti specifici quali, ad esempio, il bilanciamento tra procedure di prevenzione e maggior produttività del complesso aziendale.

Potrà, dunque, essere idoneo ed attuale quel modello "matematico"[49] apprestato da un *software* programmato con dati iniziali e capace di auto-apprendere nuove informazioni e strategie per consentire un costante adattamento del modello stesso?

A prima vista, sembra che l'adozione di un modello con tali modalità sia la soluzione migliore, posto che il calcolo statistico-matematico in cui si sostanzia gran parte del modello nonché le procedure per impedire o ridurre la possibilità di commettere reati, sono parte integrante della struttura ingegneristica dell'intelligenza artificiale.

Sulla scorta di ciò, il Legislatore potrebbe, ben presto, predisporre una regolamentazione che imponga l'adozione del modello mediante *software* di intelligenza artificiale, proprio per garantire la miglior efficacia preventiva[50].

Tale ultima considerazione porta ad interrogarsi sulle conseguenze che possano discendere, in caso di commissione di un reato presupposto, dalla dotazione di un modello 231 creato dall'intelligenza artificiale e

adottato dalla società.

- **Risvolti sulla responsabilità dell'ente per colpa organizzativa**

Per rispondere a tale ultimo quesito, occorre comprendere se l'accertamento della colpa d'organizzazione, comprovata dall'inidoneità del modello, presupponga una valutazione in termini di esigibilità di una condotta diversa.

L'assunto per cui il Giudice deve idealmente porsi al momento in cui il reato è stato commesso e sostituire il modello vigente con quello virtuoso deve, infatti, tenere sempre in debita considerazione lo stato di conoscenze tecniche e scientifiche al momento in cui è stata attuata la condotta.

Tale giudizio controfattuale, non può essere influenzato dalla conoscenza delle conseguenze della condotta posta in essere, rilevate *ex post;* pertanto, in caso di modello organizzativo redatto tramite un sistema di intelligenza artificiale, bisognerà comprendere se la società che lo ha programmato rivesta una posizione di garanzia sulla corretta gestione del *software*.

A tal fine, assumerà fondamentale rilievo il contratto di cessione del *software*.

Se tale rapporto giuridico esclude qualsivoglia ingerenza da parte del venditore, ricadrà sull'ente che lo ha acquistato il dovere di riprogrammarlo all'occorrenza o, comunque, curarne gli aggiornamenti e vigilare sullo stesso.

Diversamente, se il dominio sullo strumento *AI* rimanesse in capo al venditore, ne deriverebbe il problema di individuare una responsabilità "penale" in capo all'ente per il reato presupposto commesso da un proprio dipendente.

Infatti, la società che abbia adottato il modello *AI* avrebbe fatto quanto più sia ad essa esigibile, in base alle conoscenze tecniche e scientifiche del momento, proprio al fine avere un'organizzazione efficace in ottica di prevenzione dei reati.

Potrebbe essere obiettato che l'acquisizione di un siffatto *software* consentirebbe di affermare che questo rientri a pieno titolo nella *compliance* della società e, di conseguenza, sarebbe pur sempre ravvisabile una colpa d'organizzazione, ad esempio, per non aver predisposto un *team* specializzato nell'utilizzo e nella programmazione dei sistemi di intelligenza artificiale.

Tuttavia, in considerazione delle capacità di auto-apprendimento della macchina, gli specialisti potrebbero risultare indispensabili soltanto in ipotesi eccezionali.

Pertanto, permarrebbe la problematica di esigibilità, posto che l'ente si è affidato ad una macchina in grado di processare, con maggior precisione e continuità rispetto all'uomo, una quantità di dati infinita.

Apparirebbe, dunque, come una forzatura l'attribuzione alla società che si è dotata di tale *software* di una responsabilità da colpa organizzativa per non aver predisposto un modello organizzativo idoneo a prevenire il reato commesso.

Entrando nella logica del D.Lgs. 231/2001, la strategia che potrebbe essere adottata dal futuro Legislatore, per superare tali questioni dogmatiche, potrebbe essere quella di prevedere una speciale esenzione della responsabilità per tutti quegli enti che adottino il modello organizzativo elaborato da un *software* dotato di intelligenza artificiale, programmato appositamente per la società stessa.

Non può sottacersi però, come affermato da alcuni autori[51], che vi sarebbe il rischio di identificare uno *standard* di "organizzazione modello" definita aprioristicamente da una macchina, tramite algoritmi che si autodeterminano in base ad avvenimenti del passato.

Ulteriore pericolo è quello del cd. *automation bias*, ossia il convincimento dell'intelligenza artificiale che la sua soluzione sia l'unica corretta, convinzione che, in un settore legato al diritto penale ed alla sua interpretazione, risulta inappropriato.

In conclusione, nell'attesa di una puntuale disciplina di settore e (forse) di un ripensamento della struttura della colpa d'organizzazione, riemerge con preponderanza il rilievo dell'accettazione sociale di tale peculiare forma di innovazione tecnologica e, soprattutto, dalla relativa delimitazione dell'area del rischio consentito[52] che influenzeranno sicuramente il Legislatore nelle future scelte di politica legislativa in questa, già complessa, materia.

[1] R. Pardolesi - A. Davola, *Algorithmic legal decision making: la fine del mondo (del diritto) o il paese delle meraviglie?*, in *Questione Giustizia*, 1/2020, p. 104.

[2] A. Cadoppi-S. Canestrari-A. Manna- M. Papa, *Cybercrime*, Milano, 2023, p. 43. «*Si va dalla gestione di modelli previsionali in ogni settore, all'organizzazione della produzione e del lavoro, dalla selezione e gestione della pubblicità da indirizzare ad estese categorie od a singoli utenti (c.d. personalizzazione) a livello globale, fino alle ricerche statistiche, epidemiologiche, d'opinione, nonché a svariate funzioni di controllo "automatizzato" (ad es. in ambito fiscale), alle diagnosi e terapie mediche, agli interventi di chirurgia e microchirurgia, alla guida automatizzata di veicoli di ogni natura, comprese oggi le automobili, alla conclusione di negozi e contratti con pieni effetti giuridici, specie in ambito borsistico e finanziario, ecc.*»

[3] C. Cupelli, *La sfida dell'intelligenza artificiale al diritto penale*, in *Sistema penale*, 2023.

[4] E. Pietrocarlo, *Predictive policing: criticità e prospettive dei sistemi di identificazione dei potenziali criminali*, in *Sistema penale*, 2023. Secondo l'A. «*Tale termine si riferisce, in linea generale, all'impiego di tecniche analitiche – in particolare, quantitative – che, attraverso l'incrocio di dati, consentono di elaborare previsioni statistiche circa i luoghi di futura commissione di reati (c.d. crime hot spot) ovvero i potenziali autori o vittime, orientando le attività di polizia alla prevenzione, più che alla sola repressione del crimine. L'obiettivo ultimo è dunque quello di una riduzione del tasso di criminalità, realizzata attraverso una più razionale allocazione delle risorse e interventi mirati sui soggetti a rischio; il tutto reso possibile grazie all'analisi dei dati*».

[5]A. Cappellini, Machina delinquere non potest? *Brevi appunti su intelligenza artificiale e responsabilità penale*, in *disCrimen*, 2019; C. Piergallini, *Intelligenza artificiale: da "mezzo" a "autore" del reato?*, in Rivista italiana di diritto e procedura penale, 2020, pp. 1745 ss.; per la posizione di coloro che ritengono l'intelligenza artificiale autonomamente imputabile, nel sistema anglosassone, v. G. Hallevy, *Liability for Crimes Involving Artificial Intelligence Systems*, Dordrecht, 2015.

[6]Per un approfondimento sul tema della responsabilità nell'*autonomous driving* v. L. D'Amico, *intelligenza artificiale e auto a guida autonoma. Tra prevenzione primaria, colpa penale e rischio consentito*, in *rivista italiana medico legale*, 3/2022 p. 609; C. Piergallini, *Danno da prodotto e responsabilità penale. Profili dommatici e politico-criminali*, Milano, 2004

[7]O. Di Giovine, *Il judge-bot e le sequenze giuridiche in materia penale (intelligenza artificiale e stabilizzazione giurisprudenziale)*, in *Cassazione Penale*, fasc. 3, 2020, p. 965.

[8]F. Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *diritto penale e uomo*, 2019, p. 15.

[9]A. Formisone, *L'impatto dell'intelligenza artificiale in ambito giudiziario sui diritti fodamentali,*in *Federalismi - Rivista di diritto pubblico italiano, comunitario e comparato*, n. 22/2024, pp.114 ss.

[10] Come si legge nel rapporto CEPEJ sui sistemi giudiziairi: «*Inoltre, la neutralità degli algoritmi è un mito, in quanto i loro creatori, consciamente o meno, riversano in essi i loro sistemi di valori. Il filosofo Eric Sadin ha osservato che, dietro la loro facciata efficiente e impersonale, i sistemi algoritmici rispecchiano le intenzioni di chi li progetta o li commissiona, generando un potere operativo e asimmetrico sulla vita di altre persone. Analogamente, il ricercatore Aurélien Grosdidier ritiene che un algoritmo non sia di per sé in grado di far altro che farci afferrare, nel migliore dei casi, una parte delle intenzioni del progettista ed estende la messa in discussione all'intera sequenza del trattamento dell'informazione (intenzione del progettista, produzione del codice informatico, esecuzione di tale codice e contesto dell'esecuzione poi mantenimento). Tale rilievo è condiviso dal criminologo Aleš Zavrsnik che sottolinea che le fasi di costruzione e interpretazione degli algoritmi sono prodotte da uomini per uomini e, comunque questi ultimi siano concepiti, non possono sfuggire agli errori, ai pregiudizi, agli interessi umani e alla rappresentazione umana del mondo*».

[11]A. Cappellini, *Profili penalistici delle self-driving cars*, in *diritto penale contemporaneo rivista Trimestrale* 2/2019, p. 339. L'A. per un approfondimento sul tema del *machine learning* rinvia a H. Surden, *Machine Learning and Law*, in *Washington Law Review*, 2014, pp. 87 ss.

[12]R. Trezza, *L'Intelligenza Artificiale come ausilio alla standardizzazione del modello 231: vantaggi "possibili" e rischi "celati",* in *Giurisprudenza penale*, 2021, p. 3. L'A. ipotizza la creazione di un "modello matematico 231".

[13]G. Barone, *La regolamentazione dell'Intelligenza Artificiale: è "corsa agli armamenti"*, in *Diritto penale e processo*, 8/2024, p. 991.

[14]I 23 principi contenuti nella dichiarazione sono consultabili alla pagina web: https://futureoflife.org/open-letter/ai-principles/ tra i quali: "Responsabilità: I progettisti e i costruttori di

sistemi di AI avanzati sono soggetti interessati dalle implicazioni morali dell'utilizzo, degli abusi e azioni dell'AI, con la responsabilità e l'opportunità di plasmare queste implicazioni"; "Trasparenza giudiziaria: Qualsiasi coinvolgimento di un sistema autonomo in un processo giudiziario dovrebbe fornire una spiegazione soddisfacente e verificabile da un'autorità umana competente"; "Controllo umano: Gli esseri umani dovrebbero scegliere se e come delegare le decisioni ai sistemi di AI per raggiungere obiettivi individuati".

[15]Si tratta di un comitato che si occupa di analizzare e valutare comparativamente i sistemi giudiziari degli stati membri al fine di consentire il miglioramento dell'efficienza e della qualità della giustizia.

[16]Consultabile al link: https://rm.coe.int/0900001680993348.

[17] La Carta cristallizza cinque principi sull'utilizzo dell'AI nei sistemi giudiziari e ambiti connessi: "il principio del rispetto dei diritti fondamentali; il principio di non discriminazione; il principio di qualità e sicurezza; il principio di trasparenza, imparzialità e equità; il principio del controllo da parte dell'utilizzatore", fornendo a coloro che prendono decisioni pubbliche ed agli attori del diritto strumenti per comprendere la cd. "giustizia predittiva". Chiaramente, si preoccupa anche di valutare i rischi che dall'utilizzo di tali tecnologie possano derivare, nonché i benefici dovuti alla "trasparenza, prevedibilità e omogenizzazione della giurisprudenza". Infine, nell'invito agli Stati ed alle Organizzazioni a regolamentare il settore della "cybergiustizia", riconosce il valore primario dei diritti fondamentali dell'uomo che costituisce in ogni caso la cornice entro cui predisporre la normativa di settore.

[18]Per un miglior approfondimento della Carta etica europea per l'uso dell'intelligenza artificiale nei sistemi di giustizia penale e nei relativi ambienti v. S. Quattrocolo, *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente discussione tra scienze penali e informatiche*, in *Legislazione penale*, 2018.

[19]L'atto è consultabile nel sito della Casa Bianca al link: https://www.whitehouse.gov/ostp/ai-bill-of-rights/.

[20]Per un approfondimento della Convenzione v. C. Ciccia Romito, *Intelligenza Artificiale: la Convenzione quadro del Consiglio d'Europa,* in *Altalex*, 2024. L'atto può essere visionato al link: https://www.coe.int/it/web/conventions/new-treaties.

[21]Il regolamento è consultabile al seguente link: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=OJ%3AL_202401689. In particolare, al Considerando 1 viene dichiarato lo scopo di: *«migliorare il funzionamento del mercato interno istituendo un quadro giuridico uniforme in particolare per quanto riguarda lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di intelligenza artificiale (sistemi di IA) nell'Unione, in conformità dei valori dell'Unione, promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea («Carta»), compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, proteggere contro gli effetti nocivi dei sistemi di IA nell'Unione, nonché promuovere l'innovazione. Il presente regolamento garantisce la libera circolazione transfrontaliera di beni e servizi basati sull'IA, impedendo così agli Stati membri di imporre restrizioni allo sviluppo, alla commercializzazione e all'uso di sistemi di IA, salvo espressa autorizzazione del presente regolamento».*

[22] Per dover di cronaca è opportuno aggiungere che anche l'Italia si sta muovendo in tale direzione; infatti, è al vaglio del parlamento il disegno di legge sull'intelligenza artificiale che avrà il compito di armonizzare la disciplina dell'*AI act* europeo al nostro ordinamento giuridico, consultabile al seguente link https://www.senato.it/leg/19/BGT/Schede/Ddliter/testi/58262_testi.htm.

[23]Cfr. L. D'Amico, *intelligenza artificiale e auto a guida autonoma,* cit., p. 601. Con riguardo al settore dell'*automotive* l'A. ha, infatti, affermato che un eccessivo ricorso al principio di precauzione «*comporterebbe l'astensione dallo sviluppo di un settore che, invece, si candida a diventare il futuro della mobilità mondiale: rinunciare allo sviluppo delle ricerche in materia implicherebbe la rinuncia contestuale a tutti i potenziali benefici sociali che essa porterebbe con sé*».

[24] D'altronde, la tollerabilità del rischio sociale e la delimitazione del *rischio consentito* avrebbero, certamente, come in passato è accaduto, rallentato fortemente se non addirittura impedito lo sviluppo e l'utilizzo dell'intelligenza artificiale nei settori più eterogenei, tra cui, appunto, la giustizia predittiva. Sul punto v. A. Cappellini, *Profili penalistici delle self-driving cars*, cit. p. 332, secondo cui: «*Il concetto di rischio che viene in rilievo non è infatti un quantum assoluto, dalla sola portata probabilistico-oggettiva: ma un rischio tollerato, accettato dalla società. Esso, dunque, scaturisce da un giudizio di tipo (complessivamente) politico-valutativo, che si fonda non solo su granitici dati scientifici, ma anche sui mutevoli umori sociali, dalla più varia origine, che ne condizionano la sua percezione e percepibilità. Non si esagera, probabilmente, nell'affermare come la tollerabilità sociale di un rischio sovente affondi le sue radici più profonde non tanto nella sua dimensione oggettiva, scientifica, quanto piuttosto in deformanti pregiudizi e paure anche irrazionali, in larga parte legati fortemente al*

momento comunicativo del supposto pericolo».

[25]A. Nisco, *Riflessi della compliance digitale in ambito 231*, in *Sistema penale*, 2022, p.1. L'A., infatti, con l'espressione "*compliance digitale*" intende riferirsi agli "*effetti dell'applicazione di tecnologie emergenti ai sistemi di compliance e, tra questi, ai modelli di organizzazione e gestione previsti dal d.lgs. 231/2001*".

[26] Più precisamente si tratta di soggetti dotati di poteri di rappresentanza o di direzione dell'ente ovvero di unità organizzative con autonomia funzionale e finanziaria. Naturalmente sono equiparati a questi ultimi anche i soggetti che esercitano di fatto tali poteri, v. E. Amati - N. Mazzacuva, *Diritto penale dell'economia*, Milano, 2023, p. 47.

[27] L. Parodi*, Illecito penale dell'ente e colpa di organizzazione. Una recente conferma della traiettoria garantista tracciata dalla giurisprudenza di legittimità*, in *Sistema Penale*, 2023; Cfr. F.R. Dinacci, *La dimensione probatoria e del diritto al silenzio nella disciplina della responsabilità da reato degli enti. Verso letture "osservanti" dei principi*, in *Arch. pen.,* 1/2022, p. 12 s.; C. Piergallini, *Una sentenza "modello" della Cassazione pone fine all'estenuante vicenda "Impregilo"*, in *Sistema Penale,* 2022, p. 3; contra v. E. Amati - N. Mazzacuva, *Diritto penale dell'economia*, cit., p. 56. L'A. afferma che «*Solo nel caso in cui il reato presupposto sia commesso da un apicale è prevista inoltre una inversione dell'onere probatorio («l'ente risponde se non prova»); viceversa, nell'ipotesi di reato commesso dal sottoposto l'onere della prova della mancata adozione e dell'inefficace attuazione dei modelli organizzativi grava sull'accusa*».

[28]Cass. pen., Sez. Un., Sent., 24/04/2014, n. 38343, in *OneLegale*, «*La disciplina dei criteri di imputazione del reato all'ente in presenza di soggetto in posizione apicale non viola il principio di responsabilità della responsabilità penale, perché il rapporto di immedesimazione organica tra la persona e l'ente rende il fatto proprio dell'ente, e perché la colpa c.d. di organizzazione, consistente nel non essersi l'ente organizzato per prevenire la commissione dei reati, rende l'ente colpevole*»; Contra, G. De Vero, *Struttura e natura giuridica dell'illecito di ente collettivo*, in *Rivista Italiana di diritto e Procedura Penale*, 2001, p. 1141. L'A afferma che sarebbe sufficiente il solo riscontro del solo criterio oggettivo, ossia che l'autore del reato agisca perseguendo un interesse od un vantaggio dell'ente.

[29] E. Amati - N. Mazzacuva, *Diritto penale dell'economia*, p. 53, cit.

[30] Cass. pen., Sez. IV, Sent., 06/09/2021, n. 32899, in *OneLegale*. La Suprema corte, infatti, stabilisce che la

colpa d'organizzazione «*sul piano concettuale non coincide con l'inesistenza di un idoneo ed efficace modello organizzativo e di gestione; allo stesso modo in cui il fatto da provare non coincide con la circostanza che per presunzione legale vale a dimostrarlo. Ciò conferma la persuasività dell'affermazione secondo la quale incombe sull'accusa l'onere di dare dimostrazione della colpa di organizzazione, mentre l'ente può dare dimostrazione della assenza di tale colpa*». Nello stesso senso, Cass. pen., Sez. IV, Sentenza, 28/03/2023, n. 21704, in *OneLegale*; Cass. pen., Sez. IV, Sentenza, 15/02/2022, n. 18413, in *OneLegale.*

[31]Cass. pen., Sez. IV, Sent., 06/09/2021, n. 32899, cit. «*L'accertamento della colpa di organizzazione, che costituisce il fondamento della responsabilità dell'ente, presuppone anche una valutazione sull'idoneità del modello adottato secondo il criterio epistemico-valutativo della cd. "prognosi postuma". Ne consegue che il giudice dovrà idealmente collocarsi nel momento in cui il reato è stato commesso e verificarne la prevedibilità ed evitabilità supponendo in via controfattuale che sia stato adottato un modello organizzativo "virtuoso". Si dovrà, quindi, verificare l'attuazione del modello in termini di efficacia, mentre si deve escludere che il controllo giudiziario possa avere una portata totalizzante. Il modello, in altri termini, non dovrà essere testato dal giudice nella sua globalità*»; nello stesso senso v. Cass. pen., Sez. VI, Sent., 11/11/2021, n. 23401, in *OneLegale*.

[32] Cass., Sez. IV, Sent., 11/01/2023, n. 570, in *OneLegale*.

[33] E. Amati - N. Mazzacuva, *Diritto penale dell'economia*, p. 58, cit.

[34] Cass., Sez. IV, Sent., 11/01/2023, n. 570, cit.

[35]V. Mongillo, *Presente e futuro della compliance penale*, in *Sistema Penale*, 2022, pp. 2 e 3. In particolare, "*lo statuto penale dell'impresa poggia, nella configurazione corrente, su due gambe, nell'ottica di un sistema integrato: prevenzione e repressione, a cui si aggiunge la valvola complementare della riparazione, che ormai taglia trasversalmente i due momenti*".

[36]V. Mongillo, *Presente e futuro della compliance penale*, cit., pp. 2 e 3. L'A, dopo aver descritto le varie articolazioni della *compliance*, chiarisce che la *compliance* penale si compone della *compliance* "preventiva" e *compliance* "reattiva".

[37]R. Blaiotta R., *Diritto penale e sicurezza del lavoro*, Torino, 2023, p. 360;

[38]A titolo esemplificativo, l'art. 12 del D.Lgs. 231/2001 prevede che in caso di adozione ed operatività post factum del modello conseguirà una riduzione della sanzione da un terzo alla metà. Inoltre, se da tale adozione segue anche l'immediato risarcimento del danno la riduzione sarà compresa tra la metà ed i due terzi.

[39]R. Blaiotta, *Diritto penale e sicurezza del lavoro*, cit., p. 361.

[40]P. Severino, *Il sistema di responsabilità degli enti: alcuni problemi aperti*, in AA.VV., *La responsabilità penale degli enti,* Il Mulino, 2016, p.74;

[41] E. Amati - N. Mazzacuva, *Diritto penale dell'economia*, p. 60, cit.

[42]A. Bernasconi, *Responsabilità amministrativa degli enti (profili sostanziali e processuali)*, in *Enciclopedia del diritto*, Annali, vol. II, tomo II, Milano, Giuffrè, 2008, p. 968. L'A. riporta le parole di P. Bastia, *I modelli organizzativi,* Milano, 2005, p. 134.

[43]G.J. Scignano, *La responsabilità da reato dell'ente nel riciclaggio mediante monete virtuali*, in *Diritto penale e intelligenza artificiale "nuovi scenari"*, (a cura di) G. Balbi – F. De Simone – Andreana Esposito – S. Manacorda, Torino, 2023, p. 84.

[44]Per un miglior approfondimento dell'istituto v. S. Ricci - G. Viaciago, *L'organismo di vigilanza nelle società*, Milano, 2023; E. Di Fiorino - C. Santoriello, *Introduzione a "L'Organismo di Vigilanza nel sistema 231*, Pisa, 2021.

[45]N. Abriani, *La corporate governance nell'era dell'algoritmo Prolegomeni a uno studio sull'impatto dell'intelligenza artificiale sulla* corporate governance, in *Il nuovo diritto delle società*, 3/2020, p. 268 ss. L'A. individua i principali settori in cui si inizia ad intravedere un'interferenza tra intelligenza artificiale e *governance* aziendale, in particolare:

«*i) l'utilizzo di strumenti di IA per l'organizzazione e il funzionamento societario interno (prospettiva interna di corporate governance);*

ii) gli strumenti di IA sia come supporto sia come output dell'attività di impresa;

iii) il ricorso a strumenti di IA per la valutazione dall'esterno del funzionamento societario (prospettiva esterna dei mercati finanziari)».

[46]A. Nisco, *Riflessi della compliance digitale in ambito 231*, cit. pp. 5 e ss.

[47]A. Nisco, *Riflessi della compliance digitale in ambito 231*, cit. p. 5

[48]A. F. Tripodi, *Uomo,* Societas, Machina, in *La legislazione penale*, 2023, p. 11. L'A., per un approfondimento sul tema, cita P. Norvig, *Macchine che apprendono*, in D. Heaven (a cura di), *Macchine che pensano. La nuova era dell'intelligenza artificiale*, Bari, 2018, pp. 31 e ss.; S. Beck, *Intelligence agents and criminal law - Neglicence diffusion of liability and electronic personhood*, in *Robotics and Autonomous Systems*, 2016, pp. 138 e ss.

[49]R. Trezza, *L'Intelligenza Artificiale come ausilio alla standardizzazione del modello 231: vantaggi "possibili" e rischi "celati",* cit., pp. 3 e 4.

[50]A. Nisco, *Riflessi della compliance digitale in ambito 231*, cit. p. 10. L'A afferma che «*la pretesa di esattezza e di*

maggiore effettività, avanzata da queste tecnologie, è destinata a incidere sul formarsi di best practices e, dunque, sulla standardizzazione dei sistemi di compliance, quantomeno in alcuni settori. Il che potrebbe finire, progressivamente, col condizionare il giudizio di idoneità dei modelli organizzativi, che non adottano misure tecnologiche (ritenute non eludibili), o adottano sistemi (considerati) poco performanti».

[51]A. Nisco, *Riflessi della compliance digitale in ambito 231*, cit. p. 11;

[52]L. D'Amico, *Intelligenza artificiale e veicoli a guida autonoma*, cit., pp. 601 ss.; A. Cappellini, *Profili penalistici delle* self-driving cars, cit., p. 329.