LUISS

Dipartimento
di Giurisprudenza

Dottorato in Diritto e Impresa

Ciclo XXXVI

Criminal compliance e nuove tecnologie

Prof. Avv. Maurizio Bellacosa

RELATORE

Dott.ssa Laura Apuzzo

CANDIDATA

Anno Accademico 2023/2024

Alla mia famiglia,

INDICE

INTRODUZIONE

Le nuove tecnologie rappresentano il "motore" della c.d. industria 4.0 e sono alla base della "rivoluzione" che sta coinvolgendo tutti i settori della vita sociale ed economica.

Il presente elaborato mira ad esaminare i possibili utilizzi delle nuove tecnologie – nello specifico, *Blockchain* e Intelligenza Artificiale – nell'attività di *criminal compliance* a livello aziendale.

Il primo capitolo ripercorre i tratti salienti della disciplina della responsabilità della persona giuridica di cui al decreto legislativo 231 del 2001 partendo dall'analisi del significato del termine *compliance*.

L'introduzione nel nostro ordinamento della responsabilità degli enti ha rappresentato una fondamentale svolta ed ha determinato il superamento del principio secondo il quale *societas delinquere non potest*. Nel tempo il catalogo dei *predicate crimes* si è rapidamente esteso e con l'inserimento dei reati informatici nel Decreto 231, le imprese sono state chiamate a rispondere in modo formale all'esigenza di governare il rischio cibernetico; pertanto, nella seconda parte del primo capitolo si cercherà di capire quali siano le misure che hanno in concreto adottato.

L'analisi proseguirà con il secondo capitolo dedicato ad esaminare le caratteristiche della *blockchain* e dell'intelligenza artificiale, in primo luogo, da un punto di vista tecnico per poi passare a valutare le questioni che si pongono a livello giuridico nel momento in cui a commettere un illecito è l'agente artificiale.

La questione principale riguarda l'imputazione della responsabilità, in quanto l'evoluzione tecnologica ha determinato lo sviluppo di macchine pensanti, capaci di autoapprendere che spesso danno vita a risultati imprevedibili anche per il programmatore; in questi casi, ci si chiede quale sia la soluzione da un punto di vista giuridico passando in rassegna le ipotesi possibili e le teorie sviluppate dalla dottrina sul tema.

Il terzo capitolo sarà dedicato ad un'analisi integrata delle tecnologie e degli strumenti organizzativi presenti a livello aziendale al fine di determinare quali potrebbero essere i rischi, ma soprattutto i vantaggi per le imprese connessi all'utilizzo della *blockchain* e dell'IA.

L'esame si focalizzerà principalmente sull'ipotesi di digitalizzazione dei processi aziendali e del modello organizzativo; sull'automatizzazione del *risk assestment* e del *risk management*, cercando di capire come conciliare la c.d. *digital criminal compliance* con la tutela dei diritti dei soggetti coinvolti.

Nella seconda parte del terzo capitolo si svolgerà un'analisi casistica al fine di toccare con mano i problemi che si pongono in ambito tecnologico e i vantaggi che deriverebbero da un utilizzo massivo di strumenti come l'IA o la *blockchain.*

Infine, la parte conclusiva del lavoro sarà dedicata ad una rassegna della normativa elaborata in ambito europeo effettuando una comparazione con l'approccio adottato dagli Stati Uniti.

L'Unione Europea con l'intento di realizzare il miglior bilanciamento degli interessi in gioco ha intrapreso la strada della regolazione accentrata

approvando da ultimo (14 giugno 2023) la proposta di Regolamento sull'IA che si propone di delineare i requisiti necessari per lo sviluppo e la circolazione di strumenti che si basano sull'intelligenza artificiale.

Tale approccio differisce in parte da quello americano che invece, risulta essere principalmente incentrato su un'autoregolamentazione finalizzata a favorire un rapido sviluppo tecnologico soprattutto, per non perdere occasioni in termini di competitività con le altre potenze mondiali.

CAPITOLO I

La *criminal compliance*: la prevenzione e la gestione del rischio reato in ambito aziendale.

SOMMARIO: 1. Premessa. Cosa si intende per *criminal compliance*? - 1.1. Il fondamento della responsabilità della persona giuridica: la colpa di organizzazione. - 1.2. I criteri di ascrizione della responsabilità. - 1.3. modelli organizzativi. - 1.4. I caratteri ed i contenuti del modello. - 1.5. Il giudizio di idoneità. - 1.6. Il ruolo dell'Organismo di Vigilanza. - 2. L'esigenza di governare il rischio cibernetico. - 2.1. Le caratteristiche del reato cibernetico - 2.2. La necessità per le imprese di dotarsi di un sistema adeguato di *cybersicurezza*.

1. Premessa. Cosa si intende per *criminal compliance*?

Il termine *compliance*[1] da un punto di vista semantico non assume un significato univoco.

Sebbene a livello letterale rappresenti la conformità alle prescrizioni normative - imponendo l'ottemperanza di comandi o divieti - intesa in senso ampio assume molteplici sfaccettature.

[1] Per un esame approfondito della tematica si veda: V. MONGILLO, *Presente e futuro della compliance penale*, in *Sist. Pen*., 11 gennaio 2022, 1 ss.; A. NISCO, *Riflessi della compliance digitale in ambito 231*, in *Sist. Pen.*, 14 marzo 2022, 1 ss.; G. PRESTI, *What We Talk About When We Talk About Compliance*, in S. MANACORDA-F. CENTONZE (Eds.), *Corporate Compliance on a Global Scale. Legitimacy and Effectiveness*, Springer 2022, 25 ss.; T. ROTSCH, *Criminal Compliance – Begriff, Entwicklung und theoretische Grundlegung*, in ID. (Hrsg.), *Criminal Compliance – Handbuch*, Nomos, Baden-Baden, 2015, 41 ss.

Ad esempio, quando ci si riferisce alla *corporate compliance*, si intende il rispetto delle regole e dei protocolli interni e quindi di strumenti di autoregolazione.

Si può dire che la *compliance* più che il fine rappresenti il mezzo per gestire il rischio. La procedimentalizzazione dell'attività aziendale, la trasparenza, la tracciabilità ed il controllo consentono di definire e misurare la conformità della società alle regole previste a livello sia pubblico che privato.

Invero, quando si parla di conformità si tende a confinare l'indagine al diritto penale o a specifici settori, in realtà la *compliance* assume un ben più ampio respiro in quanto, rappresenta un metodo di gestione improntato al *risk assestment* e al *risk managment* che si prefigge - quale obiettivo ultimo - la prevenzione di determinati rischi per evitare che si verifichino eventi contrari alla legge oppure a regole autonormate.

Attenta dottrina[2] distingue almeno tre tipi di *compliance*: in primo luogo, si può avere una conformità imposta dal legislatore o dall'autorità e presidiata da sanzioni punitive; in secondo luogo, una *compliance* incentivata che si caratterizza per la premialità riconosciuta a fronte dell'adozione di idonei sistemi di prevenzione; infine, una *compliance* volontaristica i cui lineamenti sono definiti in fonti di *soft law* e che risulta essere fortemente incentivata dalle rapide trasformazioni del mercato.

[2] Sul punto si veda: V. MONGILLO, *Presente e futuro*, cit., 7 ss.

La pluralità di fonti e la complessità dei sistemi normativi ha incentivato la diffusione di un meccanismo di *compliance* cooperativo pubblico-privato, strutturato in forma prevalentemente dialogica, allo scopo di interpretare la normativa per prevenire la configurazione del rischio.

Ogni ambito organizzativo necessita di una regolamentazione che sia *compliant* con inevitabili ripercussioni sulle norme che spesso presentano punti comuni e che richiedono la realizzazione di sistemi integrati di prevenzione[3].

Inoltre, sono state introdotte delle forme privatizzate di controllo penale che si aggiungono e talvolta sostituiscono l'*enforcement* pubblico[4].

A livello internazionale sono state introdotte forme di giustizia negoziata al fine di instaurare un sistema cooperativo e non esclusivamente punitivo; si pensi alla *prosecutorial discretion* volta a far emergere illeciti aziendali tramite la richiesta da parte dell'autorità pubblica di collaborazione in cambio di benefici premiali.

A tal proposito, si può rilevare che nei sistemi di *Common Law* si stanno diffondendo nuove tecniche negoziali e meccanismi di *diversion*[5] che

[3] Sono vari i settori in cui emerge plasticamente l'esigenza di realizzare sistemi integrati: in primo luogo, si guardi al necessario raccordo tra piani prevenzione della corruzione e modelli 231, ma anche nel settore finanziario, al bilanciamento tra l'esigenza di ottemperare agli obblighi antiriciclaggio e la modellistica 231, per un approfondimento si veda V. MONGILLO, *Presente e futuro*, cit., 10.

[4] A tal proposito, si pensi alle investigazioni interne spesso introdotte in ambito aziendale per garantire la funzionalità dell'organizzazione e i diritti dei soggetti coinvolti nei vari processi.

[5] Si pensi ai *deferred prosecution agreement* di matrice statunitense, F. MAZZACUVA, *"Deferred prosecution agreements": riabilitazione "negoziata" per l'ente collettivo indagato. Analisi comparata dei sistemi di area anglo-americana*, in *Ind. pen*., 2013, 737 ss.; ID, *La diversione processuale per gli enti collettivi nell'esperienza anglo-americana*, in *Dir*.

rappresentano una forma di giustizia negoziata soprattutto per i reati che si sviluppano a livello transfrontaliero.

Quindi il termine *compliance* non assume un significato univoco, anche se la finalità perseguita risulta essere la medesima, ossia la conformità alle regole volte a prevenire il rischio di eventi infausti che - come detto - assumono un forte impatto in ambito imprenditoriale.

1.1 Il fondamento della responsabilità della persona giuridica: la colpa di organizzazione.

L'introduzione della responsabilità della persona giuridica dipendente da reato ha rappresentato il superamento del brocardo secondo cui "*societas delinquere non potest*".[6]

pen. cont. Riv. Trim., 2016, 2, 80 ss.; R. A. RUGGIERO, *Non prosecution agreements e criminalità d'impresa negli U.S.A.: il paradosso del liberismo economico*, in *Dir. pen. cont*., 12 ottobre 2015; P. SEVERINO, *La responsabilità dell'ente ex d.lgs. 231 del 2001: profili sanzionatori e logiche premiali*, Milano, 2018, 1122 ss.; R. SABIA, I. SLAVEMME, *Costi e funzioni dei modelli di organizzazione e gestione* ai sensi del d.lgs. n. 231/2001, in A. DEL VECCHIO, P. SEVERINO (a cura di), *Tutela degli investimenti tra integrazione dei mercati e concorrenza di ordinamenti*, Bari, 2016, 445 ss.

[6] Per un approfondimento sulle teorie dottrinali, precedenti all'introduzione del d.lgs. 231/2001, che si dichiaravano contrarie al mantenimento del dogma *societas delinquere non potest* si veda: F. BRICOLA, *Il costo del principio "societas delinquere non potest" nell'attuale dimensione del fenomeno societario*, in *Riv. Trim. dir. proc. pen*., 1970, 951 ss.; G. MARINUCCI, *Il reato come azione. Critica di un dogma*, Giuffrè, 1971, 175 ss.; G. DE SIMONE, *I profili sostanziali della responsabilità amministrativa degli enti: la "parte generale" e la "parte speciale" del d.lgs. 8 giugno 2001 n. 231*, in AA. VV., *Responsabilità degli enti per illeciti amministrativi dipendenti da reato*, Cedam, 2002, 73 ss.; O. DI GIOVINE, *Lineamenti sostanziali del nuovo illecito punitivo*, in (a cura di Giorgio Lattanzi) *Reati e responsabilità degli enti*, Giuffrè, 2010, 3 ss.

Orbene, il riconoscimento della capacità dell'ente di delinquere in realtà costituisce l'esito di una lunga stagione di dibattiti[7].

Il dilagare della criminalità economica aveva fatto emergere l'inefficacia di un meccanismo d'imputazione costruito esclusivamente sull'individuo[8].

Nel contesto aziendale spesso si verifica uno scollamento tra decisore ed esecutore; pertanto, può accadere che chi possiede il potere decisionale trasferisca quello gestorio e quindi non realizzi in concreto il fatto tipico. Ciò determina che il soggetto attivo si trovi a rispondere di un fatto solo per averlo realizzato mancando la dovuta conoscenza degli elementi che in ambito penale consentono l'ascrizione della responsabilità da un punto di vista soggettivo[9].

Invero, l'inadeguatezza di un sistema punitivo improntato sulla sola responsabilità della persona fisica si riflette anche sul meccanismo sanzionatorio.

---

[7] Storicamente si riteneva che la società fosse incapace di commettere un'azione in senso stretto in quanto necessariamente doveva far riferimento ad una persona fisica che agisse in virtù di un rapporto di immedesimazione organica; tra gli altri si veda G. DE SIMONE, *Societas delinquere et puniri potest, La questione della responsabilità penale degli enti collettivi tra dogmatica e politica criminale,* Como, 2000, 203 ss.; l'Autore ritiene che il dogma possa essere superato facendo riferimento a dei criteri di collegamento costruiti *ad hoc* sulla persona giuridica che consentano l'individuazione di una responsabilità personale.
Altre obiezioni che venivano sollevate riguardavano nello specifico: l'impossibilità dell'ente di sopportare l'afflittività della pena ed il contrasto con il principio di personalità della responsabilità penale; si veda tra gli altri C.F. GROSSO, voce *Responsabilità penale*, in *Nss. Dig. It.*, Utet, vol. XV, 1968, 712; C. E. PALIERO, *Problemi e prospettive della responsabilità penale dell'ente nell'ordinamento italiano*, in *Riv. Trim. dir. e proc. pen.*, 1996, 1175; C. DE MAGLIE, *L'etica e il mercato. La responsabilità penale della società*, Giuffrè, 2002.

[8] Tra gli altri si veda: C. DE MAGLIE, *L'etica e il mercato*, cit., 245 ss.

[9] Per un approfondimento sul punto: C. PEDRAZZI, *Profili problematici del diritto penale d'impresa*, in *Riv. Trim, dir. pen. econ*., 1988, 140 ss.; G. DE SIMONE, *Societas delinquere*, cit., 179 ss.

Il costo sia economico che "reputazionale" della sanzione, anche prima del d.lgs. 231/2001, veniva sopportato *in primis* dall'ente[10].

Gli illeciti posti in essere nell'interesse dell'ente sono - nella maggior parte dei casi - di tipo economico, di ciò era sicuramente consapevole il legislatore che nel fissare i termini edittali ha utilizzato un parametro diverso rispetto a quello usato per la persona fisica.

La sanzione per i reati economici è spesso di tipo pecuniario e di rilevante entità, non solo perché si tratta di una serie di fattispecie dominate dal fine di profitto, ma anche per consentire un adeguato trattamento nei confronti della persona giuridica che di fatto ne sopporta il peso.

Il vero problema è che spesso tale meccanismo di traslazione non può operare per ragioni di fatto o di diritto derivandone un paradossale aggiramento del principio di personalità della responsabilità penale e facendo ricadere la sanzione sul mero esecutore della condotta[11].

L'insufficienza di un meccanismo di ascrizione costruito esclusivamente sulla persona fisica e l'esigenza di adeguare il sistema italiano al paradigma europeo[12] sono gli elementi che hanno maggiormente spinto per il

[10] Sul tema: D. PULITANÒ, *La responsabilità "da reato" degli enti nell'ordinamento italiano*, in AA. VV., *Responsabilità degli enti per i reati commessi nel loro interesse*, Supplemento al n. 6 di *Cass. Pen.* 2003, 28 ss.

[11] Sul punto alcuni autori sottolineano come spesso gli amministratori siano solo delle 'teste di paglia' di cui l'impresa si avvale per perseguire una politica societaria criminale. Tra gli altri: O. DI GIOVINE, *Lineamenti sostanziali*, cit., 4 ss.; G. MARINUCCI, *"Societas puniri potest": uno sguardo sui fenomeni e sulle discipline contemporanee*, in *Riv. Trim. dir e proc. pen*., 2003, 1193 ss.

[12] A livello europeo il primo atto che sollecitava gli Stati membri ad introdurre dei sistemi di responsabilità per le persone giuridiche è la Raccomandazione n. (88) 18 del Comitato dei Ministri del Consiglio d'Europa.

superamento dell'ormai obsoleto dogma secondo cui: *societas delinquere non potest*.

Il superamento di tale principio ha attraversato plurime fasi, fino ad arrivare alla riforma 'epocale'[13] con cui il legislatore italiano ha adottato il d.lgs. 231 del 2001, delineando i tratti caratteristici della responsabilità amministrativa dell'ente dipendente da reato. La disciplina 231 in realtà occupa un posto di rilievo nell'ambito di quello che è stato definito il modello europeo[14] di responsabilizzazione della persona giuridica.

Sebbene sia da apprezzare lo sforzo del legislatore nel determinare le linee guida della nuova forma di illecito molti sono i punti che presentano rilevanti ambiguità e lasciano spazio all'interpretazione.

Uno degli argomenti che fin dall'introduzione del Decreto è stato al centro del dibattito concerne la natura di tale responsabilità.

Le pressioni internazionali hanno condotto l'Italia nel 2000 a ratificare la convenzione OSCE (Convenzione sulla lotta contro la corruzione dei funzionari pubblici stranieri nelle transazioni commerciali internazionali) con la l. n. 300 del 2000 che, all'art. 2, obbligava gli Stati aderenti ad adottare le misure necessarie a stabilire la responsabilità delle persone giuridiche per i reati oggetto della Convenzione che coinvolgessero funzionari pubblici stranieri.

Per un approfondimento sull'*iter* che ha condotto all'adozione di del d.lgs. 231 del 2001 si veda: G. LATTANZI, *Introduzione,* in AA. VV., *Responsabilità degli enti per illeciti amministrativi dipendenti da reato*, Cedam, 2002, 1 ss.; G. LATTANZI, *Intervento,* in AA. VV., *Societas puniri potest*, 285 ss.; D. MANZIONE, *La responsabilità amministrativa delle persone giuridiche: una soluzione opportuna o solo di "comodo"?,* in AA.VV. (a cura di G. DE FRANCESCO), *La responsabilità degli enti: un nuovo modello di giustizia "punitiva",* Giappichelli 2002, 97 ss.

[13] G. MARINUCCI, "*Societas puniri potest*", cit., 1214.

[14] V. L. FOFFANI, *Genesi e sviluppo (e prospettive future) di un modello di responsabilità degli enti nell'Unione Europea*, in D. PIVA (a cura di), *La responsabilità degli enti ex d. lgs. n. 231/2001 tra diritto e processo*, Torino, 2021, 26 ss.; R. SABIA, *Responsabilità da reato degli enti e paradigmi di validazione dei modelli*, 2022, 99 ss.

In questa sede non verrà approfondito il tema, ma per una completa analisi in merito alla responsabilità degli enti, si riassumeranno i caratteri principali del dibattito.

A tal proposito, si possono individuare tre tesi: la prima propende per la natura amministrativa[15] facendo leva sul *nomen iuris*, sul regime della prescrizione, della fusione e della scissione.

Invece, i sostenitori della natura penale[16] della responsabilità si basano sulla competenza giurisdizionale, sull'afflittività della sanzione e sul criterio soggettivo di ascrizione che richiede la colpevolezza della persona giuridica.

Infine, la teoria del *tertium genus*[17] sostenuta da buona parte della dottrina e della giurisprudenza afferma che la responsabilità della persona giuridica costituisca una forma ibrida ed abbia caratteri penali, ma anche

[15] Al momento dell'introduzione del Decreto si sono espressi a favore di una responsabilità amministrativa: M. ROMANO, *La responsabilità amministrativa degli enti, società o associazioni: profili generali*, in *Riv. soc*. 2002, 398; G. MARINUCCI, *"Societas puniri potest",* cit., 1201 ss.

[16] Tra gli autori che si sono espressi per la natura penale: E. MUSCO, *Le imprese a scuola di responsabilità tra pene pecuniarie e misure interdittive*, in *Dir. e Giust*. 2001, p. 23, 8; T. PADOVANI, *Il nome dei principi ed il principio dei nomi: la responsabilità amministrativa delle persone giuridiche*, in AA. VV. (a cura di G. DE FRANCESCO), *La responsabilità degli enti: un nuovo modello di giustizia punitiva*, Giappichelli 2004, 13 ss.; C. E. PALIERO, *La responsabilità penale della persona giuridica nell'ordinamento: profili sistematici*, in AA. VV. (a cura di PALAZZO), *Societas*, cit., 23.

[17] Sostengono questa tesi tra gli altri: D. PULITANÒ, *La responsabilità da reato degli enti: i criteri d'imputazione*, in *Riv. It. Dir. e proc. pen*., 2002, 419; G. LATTANZI, *Intervento*, in AA. VV. (a cura di PALAZZO), *Societas puniri potest*, 291; G. FLORA, *Le sanzioni punitive nei confronti delle persone giuridiche: un esempio di metamorfosi della sanzione penale?*, in *Dir. pen e proc*., 2003, 1398 ss.

amministrativi e che sulla base della giurisprudenza europea sarà considerata punitiva qualora risponda ai criteri identificativi della materia penale[18].

Alla luce dei caratteri delineati dal Decreto si ritiene che la responsabilità della persona giuridica sia di natura penale[19] o comunque che corrisponda all'accezione convenzionalmente orientata di materia penale e per tale ragione richieda una regolamentazione, che si coniughi con i principi fondamentali del diritto penale.

Un'altra questione fondamentale riguarda il tipo di rimprovero che viene mosso nei confronti dell'ente, in altre parole ci si è chiesti quale sia l'oggetto dell'attività illecita di cui la persona giuridica si è resa responsabile.

La risposta a tale quesito deve prendere in considerazione vari elementi; in primo luogo, si deve tener presente che quando si parla di persona giuridica in realtà ci si riferisce ad una pluralità di soggetti che adottano una serie di decisioni e di attività capaci di impegnare l'ente.

Infatti, la *Societas* rappresenta una mente collettiva che deve affrontare una serie di situazioni complesse e per farlo è necessario che si doti di un'adeguata organizzazione.

---

[18] Sul punto si richiamano i criteri espressi dalla Corte Edu nella sentenza Engel, si veda R. SABIA, *Responsabilità da reato degli enti e paradigmi di validazione dei modelli,* cit., 102 ss.

[19] V. MAIELLO, *La natura (formalmente amministrativa, ma sostanzialmente penale) della responsabilità: una "truffa delle etichette" davvero innocua?*, in *Riv. Trim. dir. pen. ec.*, 2002, 879 ss.; G. DE VERO, *La responsabilità penale delle persone giuridiche*, Milano, 2008, 311 ss.; M. PELISSERO, *Responsabilità degli enti*, in F. ANTOLISEI, *Manuale di diritto penale. Leggi complementari*, a cura di A. ROSSI, vol. II, 15° ed., Milano, 2022, 881 ss.

Alla base deve esserci un organigramma ben definito - rappresentativo della distribuzione delle funzioni - ed una adeguata procedimentalizzazione che consenta di prevenire il rischio di commissione di reati in ambito aziendale.

È chiaro che la persona giuridica agisce in virtù di un rapporto di immedesimazione organica, ma per farlo deve dotarsi di un adeguato apparato. Si parla a tal proposito di organizzazione dell'organizzazione.

Infatti, la prevenzione del rischio reato passa attraverso l'individuazione di una serie di regole capaci di contenere le spinte criminogene dell'impresa, che per natura persegue la logica del profitto.

Quindi, si può dire che la colpa di organizzazione[20] assuma come *target* la persona giuridica ed individui una responsabilità originaria per il modo d'essere della stessa; in altre parole, la colpa della società è nettamente distinta da quella dell'autore del reato, in quanto consiste nella

[20] La necessità di riferire l'illecito all'ente anche da un punto di vista soggettivo ha determinato per il legislatore la necessità di elaborare un criterio cucito sulla responsabilità della persona giuridica; a tal proposito nella Relazione al d. lgs. 231 del 2001, 18 ss., si possono trovare degli spunti per comprendere le origini di tale forma di colpa. Il concetto trae origine dalla tesi della *Organisationsverchulden* di K. TIEDEMAN, *Die Bebußung von Unternehmen nach dem 2. Gesetz zur Bekÿmpfung der Wirtshaftskriminalitÿt*, in *NJW*, 1988, 1169 ss. Per un esame approfondito sul tema della colpa di organizzazione si rinvia a G. DE SIMONE, *Persone giuridiche e responsabilità da reato*, cit. 182 ss.; E. VILLANI, *Alle radici del concetto di colpa di organizzazione nell'illecito dell'ente da reato*, Napoli, 2016, 80 ss.; A. F. TRIPODI, *Situazione organizzativa e colpa di organizzazione: alcune riflessioni sulle nuove specialità del diritto penale dell'economia*, in *Riv. Trim. dir. pen. ec.*, 2004, 483 ss.; C. E. PALIERO, C. PIERGALLINI, *La colpa di organizzazione*, in *La responsabilità amministrativa delle società e degli enti*, 2006, 167 ss.; ID. *Colpa di organizzazione e impresa*, in M. DONINI, R. ORLANDI (a cura di), *Reato colposo e modelli di responsabilità*, Bologna, 2013, 161 ss.; C. E. PALIERO, *La colpa di organizzazione tra responsabilità collettiva e responsabilità individuale*, in *Riv. Trim. dir. pen. ec.*, 2018, 175 ss.; A. SERENI, *La colpa di organizzazione nella responsabilità dell'ente da reato. Profili generali*, in D. PIVA (a cura di), *La responsabilità degli enti ex d. lgs. n. 231/2001 tra diritto e processo*, cit. 58 ss.

predisposizione di un apparato inidoneo a prevenire reati della specie di quello verificatosi.

Ciò che viene rimproverato all'ente è la carenza di organizzazione dell'organizzazione.

Orbene, se questo pare essere il paradigma ascrittivo della responsabilità nei confronti della persona giuridica, poco o per nulla indagato è il contenuto della colpa di organizzazione.

Quindi, se da un lato sembra chiaro che la colpa dell'ente rappresenti una categoria autonoma,[21] ci si domanda in cosa si sostanzi: è una *species* di colpa o dolo oppure rappresenta una sorta di *teritum genus*?

La questione rimane al momento dubbia e poco approfondita, ma si ritiene che costituisca un punto fondamentale di cui in primo luogo il legislatore dovrà - prima o poi - occuparsi.

1.2 I criteri di ascrizione della responsabilità.

[21] Nella *Relazione ministeriale al d.lgs. 231/2001*, par. 12, si rileva che «la colpevolezza dell'ente è intrinsecamente normativa e sfugge, pertanto, alla possibilità di scandagliare a fondo il legame psicologico con il fatto illecito».
Le Sezioni Unite della Corte di Cassazione, nel caso ThyssenKrupp (Cass. Sez. Un., n. 38343 del 24 aprile 2014) hanno sottolineato che la colpa di organizzazione ha un contenuto essenzialmente normativo rilevando che «… il legislatore orientato dalla consapevolezza delle connotazioni criminologiche degli illeciti ispirati da organizzazioni complesse, ha inteso imporre a tali organismi l'obbligo di adottare le cautele necessarie a prevenire la commissione di alcuni reati, adottando iniziative di carattere organizzativo e gestionale.
Tali accorgimenti vanno consacrati in un documento, un modello che individua i rischi e delinea le misure atte a contrastarli. Non aver ottemperato a tale obbligo fonda il rimprovero di colpa di organizzazione».

Il Decreto 231 individua una serie di criteri oggettivi e soggettivi di ascrizione della responsabilità.[22]

L'articolo 5 delinea il criterio oggettivo mentre gli articoli 6 e 7 disciplinano la responsabilità da un punto di vista soggettivo.

L'imputazione oggettiva[23] si basa sulla sussistenza di due elementi: in primo luogo, un rapporto funzionale con la persona giuridica, che consenta al soggetto agente di operare in nome della società ed in secondo luogo, un collegamento di tipo utilitaristico tra il reato e l'ente.

Se da un lato, l'autore dell'illecito deve agire in virtù di un rapporto funzionale che lo lega all'ente, in quanto ha il potere di svolgere funzioni

[22] In questa sede, i criteri di ascrizione verranno brevemente analizzati per offrire un quadro completo e per comprendere i futuri sviluppi della *compliance* alla luce delle nuove tecnologie.

[23] L'art. 5 del d.lgs. 231 del 2001 specifica i criteri oggettivi di ascrizione della responsabilità nei confronti della persona giuridica. Il Decreto non ha elencato i soggetti che possono realizzare in concreto i reati presupposto (sebbene abbia distinto il modello di ascrizione della responsabilità se il fatto è commesso da un apicale o da un sottoposto), ma il richiamo al rapporto di immedesimazione organica rende conforme la disposizione in esame all'art. 27 Cost., che esprime il divieto di responsabilità per fatto altrui; sul punto si veda: C. PECORELLA, *Principi generali e criteri di attribuzione della responsabilità*, in A. ALESSANDRI e AL. (a cura di), *La responsabilità amministrativa degli enti D. lgs. 8 giugno 200, n. 231*, p. 82 ss.; G. DE SIMONE, *La responsabilità da reato degli enti nel sistema sanzionatorio italiano: alcuni aspetti problematici*, in *Riv. Trim. dir. pen. econ.*, 2004, 675; O. DI GIOVINE, *Lineamenti sostanziali*, cit., 56 ss.; R. BARTOLI, *Il criterio di imputazione oggettiva*, in G. LATTANZI, P. SEVERINO *(a cura di), Responsabilità da reato degli enti*, vol. I, Torino, 2020, p. 186 ss.
Dubbi in dottrina ed in giurisprudenza ha suscitato l'espressione nell'interesse o a vantaggio dell'ente. L'interesse caratterizza l'azione da un punto di vista soggettivo (in quanto la persona fisica non deve aver agito contro la società), mentre il vantaggio esprime in termini oggettivi ed è valutabile *ex post* alla luce degli effetti che la condotta ha avuto in concreto.
Sul punto, per tutti si veda: N. SELVAGGI, *L'interesse dell'ente collettivo quale criterio di ascrizione della responsabilità da reato*, Jovene, 2006; C. PECORELLA, *Principi generali*, cit., 83; D. PULITANÒ, *La responsabilità "da reato"*, cit., 245; R. BARTOLI, *Il criterio di imputazione oggettiva*, in G. LATTANZI, P. SEVERINO *(a cura di), Responsabilità da reato degli enti*, vol. I, Torino, 2020, p. 186 ss.

proprie della persona giuridica spendendone il nome, dall'altro l'art. 5 al comma 1 richiede che il soggetto abbia agito nell'interesse o a vantaggio dell'ente, al fine di realizzare un interesse dello stesso.

Quindi è necessario non solo un collegamento organico/funzionale, ma anche utilitaristico; in assenza di tale utile il comma 2 dell'art. 5 precisa che la responsabilità dell'ente è esclusa quando il soggetto abbia agito al fine di realizzare suo interesse esclusivo.

Da un punto di vista soggettivo, le norme cardine del sistema 231 sono, gli articoli 6 e 7; a seconda che il reato sia posto in essere da un soggetto in posizione apicale oppure da un sottoposto.

Il Decreto individua distinti criteri di ascrizione della responsabilità, ma in entrambi i casi – ricorrendone le condizioni – acquisisce efficacia esimente l'adozione e l'efficace attuazione di un modello di organizzazione e gestione.

Il modello nel Sistema 231 assume plurime funzioni che saranno approfondite in seguito, in questa sede si anticipa che lo stesso ha valenza esimente se adottato prima della commissione del reato ed efficacia riparatoria qualora sia stato implementato *post delictum*.

Chiarito ciò, il sistema delineato dal legislatore sembrerebbe attribuire efficacia esimente all'adozione del modello solo nel caso in cui il reato sia posto in essere da un *sottoposto*.

L'articolo 7[24] del d.lgs. 231/2001 dispone che l'ente è ritenuto responsabile se la commissione del reato è dipesa dall'inosservanza degli obblighi di direzione o vigilanza; al secondo comma, però, esclude tale inosservanza a fronte dell'adozione di un modello di organizzazione e gestione idoneo a prevenire reati della specie di quello verificatosi.

Nel caso di reato posto in essere dall'apicale, l'ente andrà esente da responsabilità – ai sensi dell'art. 6 – non solo qualora abbia adottato un modello idoneo, ma anche in presenza di altri due requisiti: il primo, fa riferimento alla nomina di un organismo di vigilanza[25] ed il secondo, all'elusione fraudolenta[26] del modello da parte dell'autore del reato.

A tal proposito, ci si è chiesti se il diverso meccanismo di ascrizione della responsabilità delineato dal testo del Decreto corrispondesse ad un

[24] L'art. 7 del d.lgs. 231 del 2001 al primo comma dispone che «l'ente è responsabile se la commissione del reato è resa possibile dall'inosservanza degli obblighi di direzione e vigilanza» ed al secondo comma che l'inosservanza è esclusa se il soggetto collettivo «prima della commissione del reato ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi».

[25] Sul punto: N. PISANI, *I requisiti di autonomia e indipendenza dell'Organismo di Vigilanza istituito ai sensi del d.lgs. 231/2001*, in *Resp. amm. soc. enti*, 2008, 1, 155 ss.; V. MONGILLO, *L'organismo di vigilanza nel sistema della responsabilità da reato dell'ente: paradigmi di controllo, tendenze evolutive e implicazioni penalistiche*, in *Resp. amm. soc. enti*, 2015, 4, 83 ss., A. S. VALENZANO, *L'illecito dell'ente da reato per omessa o insufficiente vigilanza. Tra modelli preventivi e omesso impedimento del reato*, Napoli, 2019.

[26] Sul concetto di elusione fraudolenta tra gli altri si veda: A. F. TRIPODI, *L'elusione fraudolenta nel sistema della responsabilità degli enti*, Padova, 2013; ID, *L'elusione fraudolenta del modello. Ruolo e gestione ermeneutica del controverso inciso a venti anni dalla sua comparsa*, in D. PIVA (a cura di), *La responsabilità degli enti ex d. lgs. 231/2001 tra diritto e processo*, 230 ss.

meccanismo d'imputazione, che distinguesse il rimprovero mosso nei confronti dell'ente in base al "tipo" di autore[27].

Sebbene inizialmente gli interpreti abbiano sostenuto che il d. lgs. 231/2001 preveda per gli apicali una responsabilità che si fonda sull'immedesimazione organica[28] - quindi il reato della persona fisica è illecito proprio dell'ente - tale ipotesi viene in concreto smentita, in quanto al di là della diversità dei requisiti previsti dall'art. 6 e 7 ciò che rileva è l'assenza di una corretta amministrazione e di un adeguato schema preventivo, pertanto se ne deduce che il paradigma ascrittivo sia il medesimo[29] sia per il reato commesso dal soggetto posto in posizione apicale che per quello realizzato dal sottoposto.

Sul piano probatorio, l'art. 6 nel delineare la responsabilità del soggetto posto in posizione apicale esplicita che «l'ente non risponde se prova che» inducendo parte della dottrina[30] a ritenere che ci si riferisse ad un'inversione dell'onere della prova.

Secondo questa teoria, l'illecito del soggetto che riveste una posizione di comando all'interno dell'azienda a fronte della sussistenza

---

[27] Ampiamente sul tema: C. E. PALIERO, *La società punita del perché, del per come, del per cosa*, in *Riv. It. Dir. proc. pen*., 2008, 1516 ss.

[28] G. DE SIMONE, *Persone giuridiche e responsabilità da reato*, *Profili storici, dogmatici e* comparatistici, Edizioni ETS, 2012, 391 ss.

[29] C. E. PALIERO, *La società punita*, cit., 1540 ss.

[30] Sul punto si veda tra gli altri: O. DI GIOVINE, *Lineamenti sostanziali*, cit., 95: l'Autrice specifica che «invertendo l'onere probatorio, il comma 1 dell'art. 6 prevede che l'ente fornisca la prova che l'organo dirigente abbia adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e gestione idonei a tal fine»; P. FERRUA, *Il processo penale contro gli enti: incoerenze ed anomalie nelle regole di accertamento*, in G. GARUTI (a cura di), *Responsabilità degli enti per illeciti amministrativi dipendenti da reato*, Padova, 2002, 232.

dell'immedesimazione organica è ascrivibile all'ente, il quale per andare esente da responsabilità deve fornire la *probatio diabolica* della fraudolenta elusione del modello organizzativo da parte del soggetto che ha contribuito alla formulazione dello stesso; fattispecie di difficile verificazione per come costruita.

Quindi, nei confronti dell'apicale è come se esistesse una presunzione di colpa organizzativa fondata sul presupposto che il rappresentante dell'ente sia a conoscenza delle procedure e pertanto un suo illecito è illecito anche dell'ente.

Tuttavia, la giurisprudenza ha chiarito che l'art. 6[31] del Decreto individua solo un onere di allegazione, in relazione alle procedure ed alle regole di prevenzione rimanendo in capo all'accusa l'onere di provare il contestato difetto di organizzazione.

La Cassazione nella recente sentenza[32], sul caso di Viareggio, sostiene che il rimprovero che viene mosso alla persona giuridica riguarda l'assenza di un'adeguata organizzazione, sintomatica di una colpa di tipo normativo, «fondata sul rimprovero derivante dall'inottemperanza […] dell'obbligo di

[31] Le Sezioni Unite ThyssenKrupp (Cass. Sez. Un., n. 38343 del 24 aprile 2014) hanno chiarito che al di là della natura della responsabilità della persona giuridica, "l'affinità" con il sistema penale e di conseguenza il necessario rispetto dell'art. 27 della Cost. impongono di far gravare sull'accusa l'onere della prova rispetto alla carente organizzazione dell'ente, che ha facoltà di fornire prova contraria.

[32] Si veda Cass. Pen., sez. IV, 8 gennaio 2021 (dep. 6 settembre 2021), n. 32899, *Sist. Pen.*, 9 novembre 2021, con scheda di P. BRAMBILLA, *Disastro ferroviario di Viareggio: le motivazioni della sentenza della Cassazione*; V. MONGILLO, *Imputazione oggettiva e colpa tra "essere" e normativismo: il disastro di Viareggio*, in *Giur. It.*, 2022, 953 ss.

adottare le cautele organizzative e gestionali, necessarie a prevenire la commissione di reati».

Chiarito che il criterio di ascrizione della responsabilità - disegnato dal Decreto 231 - è univoco, nel corso della trattazione si cercherà di capire quale sia il ruolo assegnato ai modelli organizzativi.

1.3 I modelli organizzativi.

Il riferimento ai modelli organizzativi[33] nella disciplina 231 pone le sue basi sui *compliance programs* americani[34].

Lo scopo principale dei modelli 231 è la tipizzazione delle regole comportamentali che rispondano a determinati *standard* di eticità e siano conformi ai principi fondanti della realtà aziendale in cui vengono applicati.

[33] Per un approfondimento sui modelli 231 si veda *ex multis*: R. RORDORF, *La normativa sui modelli di organizzazione dell'ente*, in *Cass. Pen*., 2003, 6S, 79 ss.; P. IELO, *Compliance programs: natura e funzione nel sistema della responsabilità degli enti. Modelli organizzativi ex d.lgs. 231/2001*, in *Resp. amm. soc. enti*, 2006, 1, 99 ss.; C. PIERGALLINI, *La struttura del modello di organizzazione, gestione e controllo del rischio-reato*, in G. LATTANZI (a cura di), *Reati e responsabilità degli enti*, cit., 153 ss.; G. AMATO, *Il modello di organizzazione nel sistema di esonero dalla responsabilità: ragioni di una scelta prudenziale*, in *Resp. amm. soc. enti*, 2015, 2, 55 ss.; A. GULLO, *I modelli organizzativi*, in G. LATTANZI, P. SEVERINO (a cura di), *Responsabilità da reato degli enti*, vol. I, cit., 241 ss.

[34] Per un esame dei caratteri del modello organizzativo, delle similitudini e delle differenze con i *compliance programs* americani si veda l'analisi di C. DE MAGLIE, cit., 64 ss.

Il modello mira a realizzare una forma di collaborazione pubblico-privato[35], volta a determinare una sinergia capace di contrastare gli illeciti commessi in ambito imprenditoriale[36].

Il fine ultimo non è quello di eliminare il rischio reato, ma di governarlo; per far ciò, lo Stato ha dovuto prendere atto del proprio limite[37] – principalmente legato all'eterogeneità degli enti di riferimento ed alla complessità della compagine sociale – ed ha deciso di adottare un atteggiamento cooperativo che viene definito di *carrot-stick*: pertanto, l'ente che dimostri un serio impegno ed investa in prevenzione ha la possibilità di beneficiare di un premio oppure – nel nostro ordinamento – di andare esente da responsabilità[38].

---

[35] Sul punto si veda: A. GULLO, *I modelli organizzativi*, cit., in G. LATTANZI, P. SEVERINO *(a cura di), Responsabilità da reato degli enti*, vol. I, Torino, 2020, 244 ss.; F. CENTONZE, *Responsabilità da reato degli enti e "agency problems". I limiti del d.lgs. n. 231 del 2001 e le prospettive di riforma*, in *Riv. It. Dir. e proc. pen*, 2017, 946 ss.

[36]Nell'ordinamento italiano, il primo utilizzo di una forma di autonomia privata, si può riscontrare per la delega di funzioni proprio al fine di realizzare il più proficuo adempimento di obblighi giuridici, in relazione alla protezione di diritti fondamentali dei soggetti coinvolti. Sul punto si veda: A. GULLO, *I modelli organizzativi*, cit., 245 ss.; C. PEDRAZZI, *Profili problematici del diritto penale d'impresa*, in *Riv. Trim. dir. pen. econ*., 1988, 125 ss.; D. PULITANÒ, *Organizzazione dell'impresa e diritto penale del lavoro*, in *Riv. Giur. Lav*., 1985, 3 ss. Sulla delega di funzioni si veda: A. FIORELLA, *Il trasferimento di funzioni nel diritto penale*, Nardini, 1985; T. VITARELLI, *Delega di funzioni e responsabilità penale*, Giuffrè, 2006.

[37] F. STELLA, *Criminalità d'impresa: lotta di sumo e lotta di judo*, in *Riv. Trim. dir. pen. econ*., 2/3, 1998, 476.

[38] Per un approfondimento sull'approccio collaborativo pubblico-privato nella lotta alla criminalità d'impresa si veda: F. STELLA, *Criminalità d'impresa: lotta di sumo e lotta di jud*o, cit., 1254 ss.

Orbene, l'apparato disegnato dal legislatore italiano presenta similitudini e differenze con il modello americano[39].

I punti di contatto più rilevanti sono due: in primo luogo, si tratta di misure, la cui adozione non è obbligatoria, ma costituisce un onere per l'impresa che voglia avere accesso ai meccanismi premiali previsti dalla normativa; in secondo luogo, i modelli devono essere effettivi non meramente cartolari.

Per quanto riguarda le differenze si deve tener presente che nel sistema americano i programmi sono elaborati dall'ente, ma secondo i limiti ed i criteri individuati dalla legge e di fatto l'adozione del modello non consente alla persona giuridica di andare esente da pena, ma solo di accedere ad una riduzione – sostanziale – della *culpability.*[40]

Le differenze tra i due sistemi sono da ricondurre essenzialmente al diverso approccio culturale alla logica della *compliance,* che negli Stati Uniti ha avuto ampia diffusione in un panorama di condivisione da parte dei destinatari delle regole già dal XX secolo[41]; in Italia non ha avuto la stessa fortuna in quanto, le imprese manifestavano forti perplessità verso la nuova forma di

[39] I requisiti sono fissati nelle *Federal sentencing guidlines* che costituiscono la base normativa dei *compliance programs,* si veda R. HEDENDEHL, *Corporate Criminal Liability: Model Penal Code Section 2.07 and the Development in Western Legal Systems*, in *Buff. Crim*. L. R., 2000, 4, 283 ss.; J. MOORE, *Corporate Culpability Under the Federal Sentencing Guidelines*, *Arizona Law Review*, vol. 34, 1992, 764 ss.

[40] Tale differenza come evidenzia O. DI GIOVINE in *Lineamenti sostanziali,* cit., 88, dipende probabilmente dalla discendenza della *corporate liability* dalla *vicarious liability* e dal fatto che quest'ultima riservava poco spazio alla difesa della *due diligence.*

[41] Sul punto per tutti si veda: J. ARLEN, *The Law of Corporate Investigations and the Global Expansion of Corporate Criminal Enforcement*, in *S. Cal. L. Rev*., 2020, 93, 699 ss.

responsabilità e apparivano impreparate di fronte al necessario cambiamento dell'apparato organizzativo.

La valorizzazione dell'adozione del modello in una fase non solo preventiva ma anche successiva rispetto alla commissione dell'illecito è alla base del meccanismo premiale costruito dal Decreto; l'art. 12, al secondo comma prevede la riduzione della sanzione pecuniaria a fronte dell'impegno dell'ente di adottare ed implementare un modello idoneo a prevenire i reati della specie di quello verificatosi oltre ad ottemperare agli obblighi risarcitori.

Inoltre, ai sensi dell'art. 17, si chiede all'ente di eliminare le carenze organizzative al fine di sottrarsi alle sanzioni interdittive e si specifica che tale condotta può essere posta in essere anche in fase esecutiva.

Lo sviluppo di un'organizzazione improntata alla prevenzione ha trovato ampio riscontro nelle politiche messe in atto per contrastare il riciclaggio e la corruzione,[42] ma si deve sottolineare che il principio dell'idoneità dell'assetto organizzativo è alla base del diritto societario[43] a dimostrazione dell'importanza che ha assunto la logica della *compliance* per le imprese.

---

[42] Nel settore del riciclaggio il d.lgs. n. 231 del 2007 contiene gli indicatori per la costruzione di un sistema preventivo, improntato sugli obblighi rivolti ad operatori finanziari e bancari che vedono l'ente come interlocutore principale. Sul punto si veda: A. GULLO, *La responsabilità dell'ente e il sistema dei delitti di riciclaggio*, in AA. VV., *Diritto penale dell'economia*, diretto da CADOPPI-CANESTRARI-MANNA-PAPA, t. II, Utet, 2019.
Diverso è il discorso per la corruzione poiché è solo con la legge n. 190 del 2012 che ha adottato la strada della prevenzione nello specifico si pensi alle Linee Guida in materia di *whistleblowing* oppure alla gestione degli appalti.

[43] Nello specifico si veda l'art. 2381 c.c. che richiede un obbligo di adeguatezza dell'organizzazione ed una vigilanza idonea su tale sistema da parte del consiglio di amministrazione e del collegio di vigilanza (art. 2403 c.c.). Sul punto si è espressa anche la giurisprudenza di merito che ha configurato un obbligo di adozione dei modelli organizzativi ai sensi della 231 in capo agli amministratori delegati ed una responsabilità in capo a questi

Ad una prima analisi risulta che i benefici di una cultura imprenditoriale ispirata alla prevenzione siano maggiori dei costi che l'ente si trova a dover sostenere; nei prossimi paragrafi si cercherà di riassumere – seppure brevemente – quelli che sono i caratteri fondamentali dei *compliance programs* nell'ordinamento italiano per poi prospettare gli inevitabili cambiamenti che la tecnologia apporterà nel contesto imprenditoriale.

1.4 I caratteri e contenuti del modello.

La normativa rispetto ai caratteri ed ai contenuti del modello risulta essere molto esigua, lasciando molto spazio alle norme elaborate dalle Associazioni di categoria; spesso intervenute per delineare Linee guida utili alla persona giuridica nella prospettazione del *compliance program*.

Tuttavia, il Legislatore con gli artt. 6 e 7 del Decreto 231 ha delineato i caratteri e i contenuti fondamentali del modello. Per quanto riguarda i caratteri - fermo restando che l'idoneità rappresenta lo scopo ultimo del *compliance program* - è necessario che lo stesso risponda ai requisiti di adeguatezza, efficienza ed effettività.

In primo luogo, il modello deve essere adeguato[44] ciò implica che sia cucito sull'ente preso in considerazione e non risponda a schemi precostituiti.

---

in caso di commissione di un reato presupposto. Si veda sul tema per tutti: N. ABRIANI, *La responsabilità da reato degli enti: modelli di prevenzione e linee evolutive del diritto societario*, in *Analisi giuridica dell'economia*, 2012, 198.

[44] Si veda: A. ROSSI, *I piani per la prevenzione della corruzione in ambito pubblico e i modelli 231 in ambito privato*, in *Dir. pen. e proc*., *Speciale corruzione*, 2013, 45. Parte della dottrina considera l'adeguatezza un sinonimo di idoneità, per tutti si veda: S. MANACORDA,

Inoltre, deve essere effettivamente implementato[45]; quindi, non deve essere frutto di un'adozione formale che non risponda alle politiche dell'ente ed alla sua *vision*, ma deve essere effettivo da un punto dal punto di vista sostanziale.

Infine, il modello deve essere efficiente e quindi necessita di un costante aggiornamento alla luce dell'evoluzione della persona giuridica, ma soprattutto della normativa di riferimento.

Se questi possono essere considerati i requisiti fondamentali quali sono i suoi contenuti?

Sul punto gli articoli 6 e 7 sono molto laconici e lasciano ampio spazio all'elaborazione ed all'interpretazione; tuttavia, si può notare che la normativa delinea un percorso da seguire nella costruzione del modello.

Un primo punto fondamentale è la conoscenza della struttura della persona giuridica e dell'organigramma e quindi di chi fa cosa, in quanto l'ente per autorganizzarsi deve prima "conoscersi".

Nel Decreto vengono individuati vari *step* da seguire in un'ottica preventiva: la mappatura del rischio, la procedimentalizzazione, il monitoraggio dei flussi finanziari e informativi[46].

In primo luogo, l'ente è chiamato a riconoscere il tipo di rischi che potrebbero verificarsi. In base al tipo di attività svolta ed a seconda che si tratti di una

---

L'idoneità preventiva dei modelli di organizzazione nella responsabilità da reato degli enti: analisi critica e linee evolutive, in *Riv. Trim. dir. pen. econ*., 2017, 71.

[45] W. LAUFER, *Inautenticità del sistema della responsabilità degli enti e giudizio di colpevolezza*, in AA. VV., *La responsabilità penale degli enti*, 11.

[46] C. PIERGALLINI, *Paradigmatica dell'autocontrollo penale, Parte I e Parte II*; A. GULLO, *I modelli organizzativi*, cit., 254 ss.

società oppure faccia parte di un gruppo il rischio si atteggerà in maniera diversa e quindi necessiterà di un adeguamento alle caratteristiche venute in rilevo.

Un altro momento importante è costituito dall'analisi normativa.

Partendo dalla rassegna dei reati presupposto è necessario confrontarli con il *core business* dell'ente per valutare in relazione a quali illeciti si concretizzi il rischio di realizzazione.

Come sottolineato da parte della dottrina[47] non è possibile azzerare il rischio; tuttavia, è necessario stabilire un grado di tollerabilità.

Pertanto, è possibile prevenirlo e gestirlo soprattutto procedimentalizzando l'attività e stabilendo anticipatamente il "processo" da seguire, in modo da ridurre al minimo la possibilità di porre in essere reati che coinvolgano la persona giuridica[48].

Altro momento importante è costituito dall'analisi dei flussi informativi e finanziari.

L'art. 6 del d.lgs. 231/2001 si riferisce espressamente all'individuazione delle modalità di gestione delle risorse finanziarie; in realtà, nell'ottica della prevenzione di fondamentale importanza è la tracciabilità dei flussi, in quanto consente di verificare quale sia stato l'impiego delle risorse, tenendo presente che la criminalità d'impresa assume spesso carattere economico.

---

[47] V. VALENTINI, *Colpa di organizzazione e misure di compliance*, in C. FIORIO (cur.), *La prova nel processo degli enti*, Torino, 2016, 82; A. ALESSANDRI, *Diritto penale e attività economiche*, Bologna, 2010, 225.

[48] Si veda ancora sul punto A. ALESSANDRI, *Diritto penale e attività economiche*, cit., 225.

Il monitoraggio delle attività eseguito mediante la trasmissione dei flussi informativi (sebbene l'art. 6 si riferisca al solo Organismo di Vigilanza) è il fulcro attorno al quale si può dire ruoti l'intera attività di *compliance* dell'ente.

Le informazioni veicolano non solo dai vertici verso gli organi di *staff,* ma anche dal basso verso l'alto.

La comunicazione ed il raccordo tra i vari di livelli della catena è uno dei migliori "antidoti" della criminalità aziendale.

Orbene, se da un lato il Decreto fornisce degli indicatori per quanto riguarda i contenuti ed i caratteri del programma, rimane del tutto silente rispetto alla struttura dello stesso; si può dire che sul punto di fondamentale importanza siano le Linee guida delle Associazioni di categoria che intervengono a colmare tale lacuna.

Il modello consta di due parti: una generale ed una speciale. Si può dire però, che le imprese rendano ostensibile solo la prima in quanto la seconda rappresenta l'insieme delle procedure adottate dalla persona giuridica per prevenire il rischio reato e può essere articolata per processi o per fattispecie.

La Parte generale[49] costituisce una sorta di carta d'identità dell'ente, in quanto ne delinea la struttura e l'articolazione interna.

All'interno del modello si possono distinguere tre sezioni: il codice etico, il sistema di controllo interno e il sistema normativo.

[49] Per quanto riguarda la configurazione dei modelli si veda per tutti: C. PIERGALLINI, *Paradigmatica dell'autocontrollo penale, Parte I e Parte II,* cit.

Per quanto riguarda il codice etico[50] vengono delineate solo le linee di indirizzo rivolte a coloro che operano all'interno della compagine sociale; l'ente quindi deve dimostrare in maniera equivocabile la scelta per la legalità anche attraverso l'adozione di adeguate regole etiche.

Complementare al codice etico è il sistema disciplinare che enumera le sanzioni previste in caso di violazione delle condotte doverose.

Di fondamentale importanza è il sistema di controllo interno volto a determinare i principi e le procedure adottate proprio per prevenire il rischio reato. L'Organismo di Vigilanza assume un ruolo centrale, in primo luogo, per il monitoraggio dei procedimenti aziendali ed in secondo luogo, per la garanzia di osservanza del modello.

Il sistema normativo, invece, si può dire che sia costituito da una serie di regole autonormate che rappresentano un piccolo "ordinamento interno" che serve da guida ad apicali e sottoposti che operano all'interno dell'impresa.

Nella parte speciale invece, vengono elaborate le misure ritenute necessarie per prevenire la realizzazione dei reati nei settori identificati.

Dunque, chiarita la struttura di base del modello, nei prossimi paragrafi si reputa necessario porre l'attenzione sul meccanismo di validazione dello stesso e sul ruolo che assume l'Organismo di Vigilanza.

[50] Sul punto, M. CAPUTO, *La mano visibile. Codici etici e cultura d'impresa nell'imputazione della responsabilità degli enti*, in *Dir. pen. cont.*, 1/2013, 114.

1.5 Il giudizio di idoneità.

Il d.lgs. 231 del 2001 agli artt. 6 e 7 delinea il contenuto minimo del modello, ma non indica le fonti oppure le coordinate necessarie per eseguire il giudizio di idoneità.

A fronte della eterogeneità dei sistemi imprenditoriali il legislatore ha ritenuto opportuno non delineare con precisione i caratteri del *compliance program* lasciando posto però, ad ampi spazi di indeterminatezza, sovente foriera di difficoltà interpretative.

La mancanza di chiari indicatori[51]– con riferimento al modello organizzativo – ha determinato molteplici difficoltà per gli interpreti chiamati a verificare l'idoneità del presidio adottato da parte dell'ente per prevenire il rischio reato.

Le difficoltà sono dovute principalmente al fatto che per come è stato configurato l'illecito si rende necessario un percorso processuale di accertamento simile a quello adottato per la persona fisica[52]; in altri termini,

[51] Sul punto si veda: V. MONGILLO, *Il giudizio di idoneità del modello di organizzazione ex d.lgs. 231/2001: incertezze dei parametri di riferimento e prospettive di soluzione*, in *Resp. amm. soc. enti*, 2011, 3, 69 ss.; S. CAVALLINI, *Il giudizio di idoneità dei modelli organizzativi: barlumi di. Colpa nell'eterno meriggio della responsabilità in re ipsa dell'ente?*, in *Resp. amm. soc. enti*, 2015, 4, 159; V. MANES, A. F. TRIPODI, *L'idoneità del modello organizzativo*, in F. CENTONZE – M. MANTOVANI (a cura di), *La responsabilità penale degli enti*, 2016, Bologna, 138 ss.; P. SEVERINO, *Il sistema di responsabilità degli enti ex d. lgs. 231/2001*, 74.

[52] Si veda: R. SABIA, *Responsabilità degli enti e paradigmi di validazione dei modelli organizzativi*, cit., 99 ss.; l'Autrice sottolinea che l'analogia tra l'accertamento processuale realizzato per gli individui e quello eseguito nei confronti della persona giuridica rendono necessari alcuni passaggi: "i) concentrarsi sulla identificazione della condotta inosservante del soggetto collettivo – e quindi, della specifica regola cautelare violata dall'ente -; ii) specificare se l'evento-reato presupposto rappresenti la concretizzazione del rischio che tale cautela violata mirava a prevenire (c.d. causalità della colpa); iii) chiedersi se il comportamento alternativo lecito avrebbe evitato o ridotto (entro un margine accettabile) il

la natura della colpa di organizzazione e l'assimilazione dell'illecito al delitto colposo di evento avvicinano il giudizio di idoneità all'accertamento della colpa penale.

Questo rappresenta un primo ostacolo sebbene non sia il solo; infatti, si può rilevare come la mancanza di indicazioni relative ai presupposti che consentono di stabilire l'idoneità del modello in concreto, rendono arduo il compito sia per l'ente che per i giudici chiamati ad effettuare tale accertamento.

La prima considerazione da fare prende spunto dal fatto che si tratta di regole "autonormate" rispetto alle quali – si ribadisce – non esiste una normativa specifica di riferimento, basandosi il modello su quanto delineato dal legislatore a livello generale nel decreto 231 e dalle linee guida delle Associazioni di categoria; questo determina l'incertezza sulla condotta doverosa che avrebbe evitato la realizzazione dell'evento verificatosi.

In secondo luogo, risulta essere problematica l'individuazione dei presupposti in relazione ai quali il modello possa essere considerato idoneo; la maggiore difficoltà deriva – come detto – dall'esiguità di informazioni normative al riguardo.

In sede di giudizio, la verifica si articola in varie fasi[53] che sono state scandite in *primis* dalla dottrina e successivamente dalla giurisprudenza; nello

rischio di verificazione dell'illecito, nonché iv) se sussista la c.d. misura soggettiva della colpa, in termini di rimproverabilità soggettiva della violazione della regola cautelare."

[53]Sul punto si veda: F. D'ARCANGELO, *Il sindacato giudiziale sui modelli organizzativi nel contesto attuale*, in R. BORSARI (a cura di), *Itinerari di diritto penale dell'economia*, p. 351

specifico, la Cassazione recentemente ha posto fine alla c.d. saga Impregilo[54] facendo luce su plurimi profili concernenti l'idoneità del modello e chiarendo

ss.; V. MANES, *Profili di metodo nell'accertamento dell'idoneità del modello organizzativo*, in R. BORSARI (a cura di), *Itinerari di diritto penale dell'economia*, 2018, Padova, 337. Il primo passaggio da effettuare in sede di accertamento della colpa di organizzazione riguarda l'identificazione della condotta inosservante; parte della dottrina (C. E. PALIERO, voce *Colpa di organizzazione e persone giuridiche*, 76 ss.) considerava l'accertamento della colpa eseguibile solo in presenza di un modello organizzativo in quanto dall'assenza dello stesso ne derivava automaticamente un difetto organizzativo; tale assunto presenta un difetto di fondo (come osservato da O. DI GIOVINE, *Il criterio di imputazione soggettiva*, 215), l'adozione del modello costituisce un onere e non un obbligo, pertanto nessun tipo di automatismo può porsi alla base di tale accertamento (La Cassazione ha affermato che l'assenza di un modello organizzativo o la sua inefficace attuazione non sono requisiti idonei a dimostrare automaticamente la sussistenza della colpa di organizzazione, ma rappresentano degli indicatori che devono essere necessariamente provati dall'accusa: sul punto si permetta di richiamare la pronuncia Cass. Pen. sez. VI, 15 febbraio 2022, dep. 10 maggio 2022, n. 18413, con nota di L. APUZZO, in *Riv. Trim. dir. pen. ec*., 2022, 363 ss.). Il secondo passaggio attiene alla verifica della causalità della colpa (sul punto si veda: C. PIERGALLINI, voce *Colpa (diritto penale)*, Cit., 242.) si richiede che l'evento verificatosi sia proprio uno di quelli che la regola cautelare mirava a prevenire. Infine, un terzo momento prevede la verifica dell'idoneità ad evitare la realizzazione dell'illecito del comportamento alternativo lecito; quindi la capacità della condotta alternativa omessa di eliminare o ridurre il rischio di verificazione del reato (v. sul punto: C. E. PALIERO, voce *Colpa di organizzazione e persone giuridiche*, cit., 79). Per un approfondimento si veda: R. SABIA, *Responsabilità da reato degli enti*, cit., 99 ss.;

[54] La Corte di Cassazione nel 2013 aveva annullato con rinvio la sentenza che aveva affermato l'idoneità del modello organizzativo. I fatti riguardavano la commissione del reato di aggiotaggio da parte del Presidente del consiglio di amministrazione e dell'amministratore delegato della società, i quali avevano manipolato i dati forniti dagli uffici preposti, inserendoli nel comunicato stampa destinato al mercato. In questo modo avevano fornito notizie false che risultavano concretamente idonee ad alterare il valore delle azioni dell'emittente. In entrambi i gradi di giudizio era stata riconosciuta l'idoneità del modello mentre la Cassazione aveva riconosciuto la non idoneità del modello, rispetto alla prevenzione del reato verificatosi accogliendo le istanze del Procuratore Generale. In particolare, i giudici ritenevano il modello carente in relazione al controllo sulle informazioni che formavano oggetto di comunicazione al mercato; inoltre, sottolineavano che l'Organismo di vigilanza, fosse unipersonale ed affidato ad un membro dell'*internal audit*, alle dipendenze degli amministratori.

La sentenza aveva sollevato plurime critiche soprattutto, perché sembrava sposare la logica secondo la quale la verificazione del reato fosse automatica dimostrazione dell'inidoneità del modello, ma anche perché ascriveva all'OdV competenze impeditive, di cui non è titolare in concreto. L'Organismo alla luce del dato normativo assume un mero ruolo di vigilanza sull'operato altrui. Per un approfondimento sui vari passaggi di questa lunga vicenda si veda *ex multis*: C. E. PALIERO, *Responsabilità degli enti e principio di colpevolezza al vaglio della*

che dalla mancanza dello stesso non deriva automaticamente la responsabilità della persona giuridica, ma è necessario accertare l'effettiva sussistenza della colpa di organizzazione.

Orbene, risulta chiaro che nella prassi il giudice dovrà valutare l'idoneità del modello non *ex post*, ma basando l'analisi sulle conoscenze attendibili al momento della commissione della condotta.

In altre parole, dovranno essere analizzate le anomalie organizzative che hanno reso possibile la verificazione del reato presupposto e ci si dovrà domandare se fossero prevedibili in base alle regole ed alle norme presenti al momento della condotta.

Il giudice non valuterà discrezionalmente "creando" la regola, ma valuterà se la condotta alternativa a livello organizzativo fosse esigibile al momento del fatto.

Sul punto sono esigue le pronunce in cui il modello viene considerato idoneo – da ciò ne deriva uno scarso investimento da parte delle imprese in prevenzione – ma come si accennava sopra la Corte di Cassazione recentemente si è pronunciata in via definitiva sul caso Impregilo[55] ed ha chiarito alcuni punti fondamentali.

---

cassazione: occasione mancata o definitivo de profundis?, in *Soc.*, 2014, 4, 474 ss., V. MANES, A. F. TRIPODI, L'idoneità del modello organizzativo, 141 ss.; R. SABIA, *Responsabilità da reato degli enti* cit., 139 ss.; C. PIERGALLINI, *Una sentenza "modello" della Cassazione pone fine all'estenuante vicenda "Impregilo"*, in *Sist. Pen*., 27 giugno 2022.

[55] Cass. Pen., sez VI, 11 nov. 2021 (dep. 15 giugno 2022), n. 23401, in *Sist. Pen*., 20 giugno 2022.

La Suprema Corte a giugno 2022, presenta le motivazioni dell'attesa sentenza *Impregilo bis*, con la quale per la prima volta è stata riconosciuta in sede di legittimità l'idoneità del modello organizzativo.

La Cassazione ribadisce che il rimprovero che viene mosso nei confronti dell'ente si basa su un *deficit* organizzativo; quindi, la colpa assume un carattere normativo; in altre parole, viene contestata l'inadeguatezza dell'organizzazione.

Inoltre, i Giudici ribadiscono che lo schema di accertamento dell'idoneità ricalca quello seguito per il reato colposo, che vede il susseguirsi di varie fasi volte a dimostrare: lo scostamento dallo *standard* cautelare imposto, la causalità della colpa[56] ed infine, il comportamento alternativo lecito.

Su questo ultimo punto – sebbene in modo non estremamente chiaro – i giudici specificano che si deve accertare che la condotta doverosa omessa potesse effettivamente evitare la verificazione dell'illecito[57].

Orbene, se da un lato risulta chiaro che il controllo dovrà essere effettuato *ex ante* - secondo il meccanismo epistemico-valutativo della prognosi postuma - si deve riscontrare che il modello sconta la mancanza di una formale validazione che avrebbe consentito al giudice, ma in *primis* all'ente, di avere uno schema da seguire e di basarvi la propria organizzazione.

[56] La Corte specifica che sarà necessario dimostrare che vi sia «corrispondenza causale tra la violazione della regola cautelare e la produzione del risultato offensivo» in quanto quest'ultimo deve corrispondere «proprio a quel pericolo che la regola cautelare violata era diretta a fronteggiare».

[57] Sul punto R. SABIA, *Responsabilità degli enti*, cit.

La Cassazione nella sentenza Impregilo, ponendosi in controtendenza rispetto alla prassi precedente, sembra valorizzare le linee guida delle associazioni di categoria, che rappresentano – secondo i giudici – un importante paramento di riferimento per delineare i requisiti di idoneità del modello.

Per la prima volta, in sede di legittimità, viene data importanza a fonti di *soft law*, non vincolanti, ma fortemente orientative in tale settore; la Corte, infatti, sostiene che nella predisposizione dei modelli organizzativi tali linee guida delineando "le caratteristiche fondamentali dei modelli per le diverse categorie di imprese", siano per l'autorità giudiziaria "un importante parametro di riferimento sebbene non vincolante".

I giudici sembrano costituire una sorta di presunzione relativa di idoneità del modello conforme alle linee guida di categoria; infatti, la corte afferma che "in presenza di un modello organizzativo conforme a quei codici di comportamento, il giudice sarà tenuto specificamente a motivare le ragioni per le quali possa ciò nonostante ravvisarsi la colpa di organizzazione dell'ente, individuando la specifica disciplina di settore, anche di rango secondario, che ritenga violata o, in mancanza, le prescrizioni della migliore scienza ed esperienza dello specifico ambito produttivo interessato dalle quali i codici di comportamento ed il modello con essi congruenti si siano discostati, in tal modo rendendo possibile la commissione del reato".

Sul punto si può notare come i giudici – sebbene riconoscano la non vincolatività delle linee guida – facciano gravare sul giudice che intenda

riconoscere l'inidoneità del modello nonostante la conformità ai codici di comportamento un onere di motivazione rafforzato.

Ad ogni modo, la pronuncia richiamata costituisce un faro[58] in tema di idoneità del modello organizzativo, che sicuramente verrà presa ad esempio dalla giurisprudenza successiva, che si troverà a giudicare l'adeguatezza dello schema preventivo adottato.

La sentenza sul caso Impregilo rappresenta un notevole passo avanti; tuttavia, non si può dire che sia risolutivo, in quanto come specificato le regole non assumono carattere vincolante ed una conformità alle stesse non fornisce una "patente di idoneità" del modello. Si può quindi ritenere che sia un punto di inizio che necessita di una prosecuzione e di un maggiore sforzo – soprattutto legislativo – per consentire ai giudici, ma in particolar modo alle imprese, di avere un parametro chiaro che garantisca l'impunità qualora sia stato pedissequamente rispettato.

1.6 L'Organismo di Vigilanza.

L'art. 6, comma primo, lett. b) del d.lgs. 231 del 2001 tra le misure da adottare per la prevenzione dei *predicate crimes* prevede l'istituzione di un Organismo

[58] C. PIERGALLINI, *Una sentenza "modello" della Cassazione pone fine all'estenuante vicenda Impregilo,* cit.

di Vigilanza[59]. Le principali funzioni assunte dal suddetto organo sono dirette a controllare l'efficace attuazione[60] del modello organizzativo.

Il decreto si presenta estremamente laconico rispetto alla disciplina dell'OdV, lasciando spazio alle interpretazioni più disparate e spesso contraddittorie della dottrina e della giurisprudenza.

L'art. 6[61] attribuisce all'Organismo autonomi poteri di iniziativa e controllo, sottolineando la funzione di vigilanza sull'osservanza e l'implementazione del modello.

Per svolgere i propri compiti è fondamentale che disponga di un *budget* adeguato e - come previsto espressamente dalla lettera d) dell'art. 6 - vi siano costanti flussi informativi da e verso l'OdV.

La normativa non chiarisce quale debba essere la composizione, la qualifica oppure i poteri dei componenti[62].

---

[59] Per un approfondimento sulla figura dell'Organismo di vigilanza si veda: A. DE NICOLA, *L'organismo di vigilanza 231 nella società di capitali*, Torino, 2015; P. IELO, *Compliance Programs: natura e funzione nel sistema della responsabilità degli enti. Modelli organizzativi e d.lgs. 231/2001*, in *Rivista 231*, 2006, 1, 99 ss.; N. ABRIANI, F. GIUNTA, *L'organismo di vigilanza previsto dal d. lgs. 231/2001. Compiti e funzioni*, in *Rivista 231*, 2012, III, 191 ss.; V. MONGILLO, *L'Organismo di vigilanza nel sistema della responsabilità da reato dell'ente: paradigmi di controllo, tendenze evolutive e implicazioni penalistiche*, in *Rivista 231*, 2015, 4, 83 ss.

[60] M. RONCO, E. MEZZETTI, *Diritto penale d'impresa*, Bologna, 2009, 69.

[61] Art. 6 d. lgs. 231/2001 stabilisce al comma 2 lett. d), che i modelli devono rispondere all'esigenza di "prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli".

[62] La laconicità delle direttive normative sul punto ha condotto a soluzioni disparate nella prassi aziendale. Si veda: A. DE NICOLA, *Il diritto dei controlli societari*, Milano 2010, 91 ss.

L'unico punto fermo è il ruolo che assume in relazione al modello organizzativo, ma sono state le Linee Guida delle Associazioni di categoria e la prassi a colmare le lacune ed a prospettare la regolazione dell'OdV.

Orbene, la prima questione riguarda la figura deputata a svolgere il ruolo di vigilanza.

Sul punto si sono contrapposti i sostenitori della natura interna dell'Organismo[63] e coloro che ritengono che una maggiore indipendenza possa essere assicurata dalla costituzione di una figura *ad hoc*[64].

Quest'ultima soluzione sembra da preferire, in quanto volta a garantire una maggiore autonomia di valutazione in ordine al funzionamento ed all'efficacia del Modello[65].

La seconda questione riguarda la composizione dell'Organismo e nello specifico se debba essere composto da un unico soggetto, oppure sia necessaria la collegialità.

[63] In tal senso si veda: A. BERNASCONI, *Art. 6*, in A. PRESUTTI – A. BERNASCONI – C. FIORIO, *La responsabilità degli enti*, Padova, 2008, 118; G. ZANALDA – M. BARCELLONA, *Responsabilità amministrativa delle società*, Milano, 2002, 72.

[64] Tra gli altri: R. CLARIZIA – E. NATI, *La responsabilità amministrativa delle persone giuridiche: il d. lgs. 231/01 tra principi generali dell'ordinamento e nuovi organi societari*, in *Giur. Comm*., 2002, 306.

[65] Si veda *Relazione al d. lgs. 8 giugno 2001, n. 231*, 3.4, in *Guida dir*., 2001, 36.

Nelle imprese medio-grandi si ritiene che sia preferibile la composizione collegiale[66], formata da soggetti esterni, ma potendo contare sull'inserimento di un interno che faccia da cesura con la persona giuridica[67].

Un altro importante aspetto riguarda i caratteri dell'OdV che sono desumibili dal quadro normativo ed interpretativo e sembrerebbero essere: l'onorabilità e la professionalità, l'autonomia e l'indipendenza e la continuità d'azione.

L'onorabilità e la professionalità sono requisiti richiamati nel settore bancario e finanziario e la loro presenza è necessaria per l'Organismo in quanto sono volti a garantire una competenza pregressa e l'assenza di provvedimenti giudiziari che potrebbero minare l'efficacia del ruolo.

Invece, il secondo binomio - indipendenza e autonomia - è funzionale all'assenza di potenziali conflitti di interesse ed a garantire la continuità d'azione, stabilendo dei flussi informativi da e verso l'Organismo.

Infine, un argomento di particolare importanza da richiamare in questa sede, riguarda il riconoscimento nei confronti dell'OdV di una posizione di garanzia[68].

Sul punto non sussiste un'opinione unanime in quanto – come si è visto il legislatore ha lasciato ampio spazio all'interpretazione – tuttavia, da

---

[66] A. DE NICOLA, *L'organismo di vigilanza 231 nella società di capitali*, Torino, 2015, 50; E. BERTOLLI, *L'organismo di vigilanza ex d. lgs. 231/2001 nella dottrina e nella giurisprudenza*, in *Rivista 231*, 2010, I, 61.

[67] Si veda C. FRIGENI, C. PRESCIANI, *L'organismo di vigilanza*, in *Compliance. Responsabilità da reato degli enti collettivi*, (a cura di) D. CASTRONUOVO, G. DE SIMONE, E. GINEVRA, A. LIONZO, D. NEGRI, G. VARRASO, Milano, 2019, 262.

[68] Per tutti si veda A. GARGANI, *Posizioni di garanzia nelle organizzazioni complesse: problemi e prospettive*, in *Riv. Trim. dir. pen. econ*., 2017, 508 ss.

un'attenta analisi della normativa emerge che l'Organismo sia una sorta di "guardiano dell'efficacia del modello"[69].

Le funzioni svolte dall'OdV ruotano attorno al modello garantendone un costante aggiornamento ed assumendo poteri di iniziativa e controllo, sempre finalizzati al funzionamento dello stesso.

Orbene, si potrebbe dire che l'Organismo non assume una posizione di garanzia in quanto qualsiasi tipo di provvedimento impeditivo, deve essere adottato da coloro che svolgono una funzione operativa all'interno dell'impresa[70].

Alla luce del quadro rappresentato, il presente lavoro cercherà di capire quale sarà il ruolo delle nuove tecnologie non solo nella prospettazione del modello, ma anche per la concreta attuazione dello stesso con significativi riflessi anche sull'attività dell'OdV.

2. L'esigenza di governare il rischio cibernetico.

Lo sviluppo di tecnologie informatiche sempre più avanzate ha alimentato, in dottrina e giurisprudenza, il dibattito relativo al potenziale meccanismo evolutivo delle categorie giuridiche a fronte delle nuove esigenze di tutela.

---

[69] A. ALESSANDRI, *La vocazione penalistica dell'ODV e il suo rapporto con il modello organizzativo*, in AA. VV., *I controlli societari*, 442.

[70] In tal senso: C. PEDRAZZI, *Corporate governance e posizioni di garanzia: nuove prospettive?*, in AA. VV., *Governo dell'impresa e mercato delle regole. Scritti giuridici per Guido Rossi, II*, Giuffrè, 2002, 1375; A. S. VALENZANO, *L'illecito dell'ente*, cit., 24; A. ALESSANDRI, *La vocazione penalistica dell'ODV*, cit., 110; F. CENTONZE, *Controlli societari e responsabilità penale*, Giuffrè, 2009, 412.

Il rapporto tra diritto penale e tecnologie informatiche è stato oggetto di interventi da parte di autorevoli organismi internazionali[71], che hanno dato luogo a normative spesso disorganiche e frammentarie.

Nel tempo si è passati da un concetto di rete legato esclusivamente ai supporti tecnici alla base di fenomeni tecnologici (cavi, fibre ottiche, processori, *software* etc.) al c.d. *Cyberspace*, riferibile allo spazio dinamico in cui si sviluppa la tecnologia.

Il termine cibernetica deriva dal greco *kyber*[72], che significa timoniere, pilota ed è stato scelto per rappresentare la scienza che studia i meccanismi con cui uomini, animali e macchine comunicano con l'ambiente esterno e lo controllano.

Il passaggio ad un Rete globale (*web* – rete di reti), getta le basi per la realizzazione di uno spazio cibernetico in cui non è più sufficiente parlare di *Computer crime*, ma è necessario riferirsi al *Cybercrime*.

I reati informatici - introdotti dal legislatore del 1993 - erano pensati per punire condotte realizzabili in sistemi chiusi, eventualmente connessi a reti il cui accesso era consentito a singole categorie di utenti. L'apertura di *Internet* al pubblico ha ampliato la capacità di delinquere attraverso la rete ed ha

[71] In materia si sono espressi: l'OCSE, il Consiglio d'Europa, il WTO, l'ONMPI, il G8 e le Nazioni Unite, ma anche i legislatori dei singoli Stati, sul punto si veda: U. SIEBER, *The International Handbook on Computer Crime. Computer-related Economic Crime and the Infrigements of Privacy*, John Wiley Sons, New York, Brisbane, Toronto, Singapore, 1986.

[72] L. PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in *Cybercrime*, Milano, 2019, 39 ss.

moltiplicato gli attacchi cibernetici, facendo emergere l'esigenza di predisporre nuove forme di tutela[73].

Sono varie le novità che emergono a fronte di questo cambiamento: in primo luogo, si assiste ad una forte estensione delle varietà di condotte e delle tecniche di commissione dei reati cibernetici.

Poi si deve sottolineare come si estendano i beni giuridici da tutelare, ma anche la platea dei soggetti - vittime potenziali - da proteggere in quanto molto spesso di fronte alle opportunità del *web* si ignorano i rischi che il suo utilizzo comporta.

Quando si parla di *cyberspazio* emergono beni giuridici quali ad esempio, la riservatezza informatica[74], da intendersi quale spazio informatico in cui il soggetto deve essere lasciato libero da intrusioni da parte di terzi, tale interesse deve essere distinto dalla *privacy* che assume il significato più generale, di diritto alla tutela dei propri dati personali. Le informazioni riferibili ad un soggetto, anche se oggetto di comunicazione devono essere controllabili dallo stesso.

[73] La "rivoluzione cibernetica" ha avuto un forte impatto sul diritto penale – sul punto L. PICOTTI, *Reati informatici*, cit., 1 ss. – il primo elemento da considerare riguarda il passaggio dai *Computer Crimes* ai *Cybercrimes*. Nel primo caso sono fattispecie tipizzate che contengono un esplicito riferimento alle nuove tecnologie dell'informazione o della comunicazione (in varie forme, ad esempio: i mezzi, la condotta, agli effetti, oppure elementi a carattere circostanziale), nel caso dei reati cibernetici si tratta di condotte che possono essere realizzate in Rete, ma quest'ultima non necessariamente risulta richiamata dal testo normativo essendo desumibile in via interpretativa (ad esempio: il riciclaggio, l'estorsione, la diffamazione, la violazione dei diritti di autore ecc.).

[74] L. PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, cit., 52 ss.

Le nuove tecnologie consentono una raccolta più veloce e penetrante dei dati, ma questo vantaggio deve essere associato ad un controllo capillare rispetto al loro utilizzo.

Nel *cyberspazio* viene in rilievo anche la sicurezza informatica, che non solo è strumentale alla tutela di altri beni giuridici, ma assume un'autonoma protezione giuridica in quanto si pone a garanzia di tutti gli interessi e diritti che si esercitano nello spazio virtuale.

Tale interesse spesso diviene indisponibile per gli stessi titolari del sistema informatico, in quanto è un bene collettivamente condiviso in forza della stretta interdipendenza che hanno i rapporti e le attività in rete[75].

2.1 Le caratteristiche del reato cibernetico.

Il passaggio dal reato informatico a quello cibernetico ha determinato il ripensamento di nozioni di teoria generale del reato – ad esempio, i concetti di "azione", "evento" e "nesso causale" – che vanno rilette alla luce delle caratteristiche del nuovo spazio digitale[76].

L'utilizzo di sistemi informatici per commettere porzioni rilevanti del "fatto tipico", su cui si fonda l'applicazione della sanzione penale, rende necessaria l'indagine sul grado di responsabilità del soggetto utilizzatore o titolare dello

[75] L. PICOTTI, *Reati informatici, riservatezza, identità digitale, Contributo AIPDP,* 1 ss.

[76] In questa prima parte verranno solo accennate le questioni che pone l'avvento e lo sviluppo della tecnologia, successivamente si approfondiranno le caratteristiche del *cyberattack* e le modalità con le quali l'ente potrà prevenire o arginare gli effetti malevoli per l'impresa.

stesso; in altri termini, l'utilizzo di sistemi intelligenti ed automatizzati pone il problema di come ricollegare "l'azione della macchina" alla volontà dei soggetti umani che se ne servono.

Inoltre, l'automazione della circolazione e della permanenza dei dati e dei contenuti in rete incide sul momento di consumazione del reato commesso in tutto o in parte nel *cyberspazio*.

Le categorie giuridiche generalmente utilizzate per determinare il momento consumativo del reato si dimostrano, quindi inadeguate di fronte agli illeciti commessi nello spazio virtuale. In questi casi il fatto si prolunga nel tempo e va oltre la c.d. perfezione formale, in quanto l'interruzione degli effetti dello stesso necessita dell'intervento dell'uomo o di specifiche tecniche.

Pertanto, la scelta del mezzo tecnologico implica un prolungamento dell'evento cibernetico[77] con tutti gli effetti che ne derivano in termini di applicazione della legge penale e prescrizione.

Nel *cyberspazio* anche il luogo di commissione del reato – che coincide con il luogo di consumazione – sembra debba riferirsi a quello della perfezione formale, che si identifica con quello della prima manifestazione dell'evento come avviene nel caso dei reati permanenti.

Queste considerazioni devono essere riviste nel momento in cui il reato assume caratteri di ubiquità, che rendono impossibile la determinazione del luogo di commissione del reato e pertanto questo coincide con quello

[77] Per un esame approfondito del tema si veda: L. PICOTTI, *Reati informatici, riservatezza, identità digitale*, cit., 15 ss.

"dell'ultimo luogo in cui è avvenuta parte dell'azione e dell'omissione" (art. 9, comma 1, c.p.p.).

Orbene, il cambiamento del contesto in cui l'illecito si realizza comporta delle modifiche, che pervadono tutti gli ambiti del diritto penale, che si ispira ai principi di stretta legalità e di colpevolezza, i quali richiedono la configurazione di una responsabilità esclusivamente per fatto proprio dell'autore; nel corso del presente lavoro si cercherà di capire come sfruttare al meglio i vantaggi delle nuove tecnologie rispettando i diritti fondamentali dei soggetti coinvolti e le regole disposte dal diritto penale.

2.2 La necessità per le imprese di dotarsi di un sistema adeguato di *cybersicurezza*.

I reati informatici – nel momento in cui sono stati inseriti nel catalogo dei *predicate crimes* – richiedono l'attuazione di un sistema di gestione che configuri un processo idoneo ad intercettare le aree in cui il rischio di realizzazione di tali reati si manifesti.

Lo sviluppo di un processo volto a garantire la sicurezza cibernetica coinvolge, non solo l'aspetto tecnologico, ma trasversalmente anche il fattore umano e le procedure che lo caratterizzano[78].

[78] Sul tema per tutti si veda F. DI MAIO, *Prevenzione e dissuasione dei reati informatici nel modello organizzativo*, in *Cybercrime e responsabilità da reato degli enti: prevenzione, modello organizzativo e indagini preliminari* (a cura di) ANDREA MONTI, Milano, 2022, 149 ss.

Infatti, la digitalizzazione dell'impresa e dei processi ha reso necessaria l'implementazione di sistemi di gestione della sicurezza delle informazioni che assumono diversi ruoli all'interno dell'organizzazione, in quanto mirano a proteggere il patrimonio informativo, a governare i processi di protezione dei dati personali ed a prevenire i reati di cui al d.lgs. 231 del 2001.

A tal fine, si può osservare che il processo di sicurezza non sviluppa una sola funzione, ma si propone di gestire la "sicurezza" intesa come bene che coinvolge tutta l'organizzazione e si pone a tutela dei rischi presenti nei processi dell'*Information Technology*.

Quindi la sicurezza delle informazioni non assume solo un aspetto tecnologico, ma pervade trasversalmente i processi, le procedure e le regole organizzative tenendo conto inevitabilmente del fattore umano.

Per quanto riguarda nello specifico l'aspetto preventivo rispetto ai reati informatici, il d.lgs. 231 del 2001[79] individua una serie di fattispecie per le

[79] L'art. 24 del d.lgs. 231 del 2001 individua essenzialmente tre categorie di massima: il primo gruppo (artt. 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater e 635-quiquies) sanziona l'accesso abusivo a sistema informatico, l'intercettazione o l'interruzione di dati tramite l'istallazione di *software* ed *hardware* specifici; il secondo gruppo (artt. 615-quater e 615-quinquies) anticipa la soglia di tutela criminalizzando la mera detenzione e diffusione di codici informatici o *hardware* idonei a consentire la realizzazione dei reati inclusi nel primo gruppo; infine, un terzo gruppo (artt. 491-bis e 640-quinquies) mira a tutelare l'integrità dei documenti informatici e degli strumenti di autenticazione mediante la firma digitale.
Nel 2019 è stata inserita nel novero dei reati informatici presupposto della responsabilità della persona giuridica, un'altra categoria di reati, che si riferisce ai soggetti che ricadono nel "Perimetro di Sicurezza Cibernetica Nazionale" e che delineano una posizione di garanzia, dal carattere pubblicistico, contenuta nel d. l. 21 settembre 2019 n. 105, convertito in legge il 19 novembre 2019 n. 133 recante *Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina nei poteri speciali nei settori di rilevanza strategica*, prevendendo uno specifico reato all'art. 1 comma 11.

quali la costruzione di un adeguato sistema di sicurezza delle informazioni consente di anticipare la soglia di protezione soprattutto sviluppando un processo dinamico di analisi del rischio, l'adozione di misure organizzative, presidi tecnologici, procedimenti ed interventi che indirettamente incidono sulla formazione, sull'informazione e sulla consapevolezza delle persone che collaborano nel contesto aziendale.

Nella costruzione di un adeguato sistema di gestione della sicurezza - intesa in senso lato - un primo aspetto da considerare riguarda in primo luogo la natura dei processi di protezione delle informazioni, dei sistemi e delle reti; in secondo luogo, l'esigenza di costruire un modello organizzativo completo, che consideri l'intera organizzazione consentendo la gestione del rischio e l'emersione di elementi sintomatici di eventi critici.

Il sistema di gestione si deve basare su un metodo efficace che facendo leva sugli attori e sugli strumenti predisposti possa garantire la sicurezza dei dati e delle informazioni aziendali.

In primo luogo, il modello deve poter contare sull'approvazione dei vertici organizzativi, in quanto il sistema esige rispetto da parte di tutti i livelli aziendali essendo parte integrante del *business* dell'impresa ed incarnando un elemento essenziale della politica decisionale dell'ente.

Per un'effettiva implementazione è necessario che sussista una netta separazione dei ruoli e delle responsabilità e che tale organigramma sia comunicato all'esterno.

Un meccanismo in cui ci sia confusione dei ruoli incorrerebbe facilmente in situazioni di conflitto di interesse e non garantirebbe la necessaria terzietà ed efficacia del modello.

Un altro punto fondamentale è rappresentato dal controllo dei diritti di accesso e di utilizzo dei sistemi e delle informazioni[80], in modo da garantire un utilizzo dei sistemi aziendali solo per lo svolgimento dei compiti relativi alle proprie funzioni.

È necessario regolamentare gli accessi al sistema, ma soprattutto le mansioni ed i procedimenti per i quali sia consentito, stabilendo un ciclo di vita che preveda l'abilitazione e la disabilitazione in ragione dei ruoli assunti all'interno dell'azienda.

Questo passaggio è fondamentale perché l'effettività del modello passa anche attraverso la trasparenza e la possibilità di ripercorrere i passaggi che compongono i vari processi; una funzione essenziale è quella di controllo interno che per essere effettiva deve essere strutturata su più livelli in modo da bilanciare i vari interessi e da garantire il corretto sviluppo dell'attività.

L'esigenza di realizzare un sistema di *Information Security* pone al centro l'analisi del rischio e la sua gestione, identificando i beni da proteggere, le minacce e le vulnerabilità cui sono esposti.

[80] Tale attività nel mondo anglosassone viene definita *least privilege*; per un approfondimento sul tema si veda F. DI MAIO, *Prevenzione e dissuasione dei reati informatici nel modello organizzativo*, cit., 160 ss.

La gestione del rischio assume carattere tecnico-funzionale e non ha ad oggetto il solo aspetto tecnologico, ma anche il fattore umano che spesso si pone alla base degli incidenti che coinvolgono i dati e le informazioni.

Il sistema di sicurezza mira a garantire che la triade Disponibilità-Integrità-Riservatezza non venga compromessa, consentendo il corretto sviluppo dei processi aziendali e prevenendo il rischio di verificazione dei *predicate crimes* in generale e dei reati informatici in particolare.

CAPITOLO II

Intelligenza artificiale e *blockchain*. Prospettive e rischi per il sistema penale.

SOMMARIO: 1. Premessa. Una prima definizione di intelligenza artificiale. - 1.1 Dai sistemi esperti ai sistemi intelligenti. - 1.2 La base della ricerca algoritmica. I *Big Data*. - 1.3 I reati commessi tramite i sistemi di IA. - 1.3.1 L'algoritmo come autore del reato. - 2. Le caratteristiche della *Blockchain*. - 2.1 Le tecnologie a registro distribuito. - 2.2 Gli *Smart Contracts*. La validazione ed il valore probatorio dei documenti salvati in *blockchain*. - 3. L'IA ed il sistema penale. - 3.1 L'imputazione della responsabilità per azioni della macchina. - 3.1.1 L'ipotesi di una responsabilità diretta dell'agente artificiale. - 3.1.2 La responsabilità colposa dell'operatore per comportamenti autonomi della macchina: l'*explainability*. - 3.1.3 Soluzioni prospettabili per il *responsability gap*.

1. Premessa. Una prima definizione di intelligenza artificiale.

La nascita dell'Intelligenza artificiale viene collocata nel 1950, quando Alan Turing pubblica il conosciutissimo *Computing machinery and intelligence*, in cui descrive il *test* da lui ideato con l'obiettivo di stabilire se una macchina fosse capace di pensare come un essere umano.[81]

Il fenomeno però, inizia a svilupparsi già nell'Ottocento con la nascita delle prime macchine programmabili e degli studi eseguiti su questi dispositivi al fine di elaborare degli algoritmi capaci di calcolare sequenze numeriche.

[81] A. TURING, *Computing Machinery and Intelligence*, in *Mind*, LIX, 1950, 433 ss.

È complesso trovare una definizione che esprima tutte le caratteristiche dell'IA, ma si ritiene che la più accreditata sia contenuta in un documento della *Stanford University* che sostiene che la stessa sia accomunabile ad "un insieme di tecniche computazionali che vengono ispirate – pur operando tecnicamente in maniera diversa – dal modo in cui gli esseri umani utilizzano il proprio sistema nervoso e il proprio corpo per sentire, imparare, ragionare ed agire"[82].

Ci si è chiesti se tale definizione fosse utilizzabile in ambito giuridico - date le peculiarità del diritto - che richiede termini e concetti chiari, comprensibili e capaci di orientare i comportamenti della collettività in modo da determinare cosa è possibile fare e cosa no.

L'intelligenza artificiale viene utilizzata in moltissimi campi e può assumere plurime sfaccettature; si può dire che non sia una disciplina unica, ma un insieme di tecniche e metodi applicati ad una molteplicità di obiettivi scientifici; pertanto, secondo parte della dottrina[83], l'interpretazione giuridica dell'IA deve essere teleologica in modo da chiarire quali siano i rischi e le opportunità dei sistemi intelligenti.

Sebbene l'intelligenza artificiale assuma plurimi significati, si può dire che la sua funzione fondamentale sia quella di utilizzare degli algoritmi che possano

[82] Si fa riferimento alla definizione data da JOHN MCCARTHY, *What Is Artificial Intelligence, rapp. Tecn.*, Stanford University, 2007. Testo originale: "[AI] is the science and engineering of making intelligence machines, especially intelligent computer programs. It is related to similar task of using computers to understand human intelligence, but AI does not have confine itself to methods that are biologically observable".

[83] G. SARTOR, *L'intelligenza artificiale e il diritto*, Torino, 2022.

emulare l'intelligenza umana coadiuvandola e talvolta sostituendola al fine di raggiungere determinati obiettivi.

1.1 Dai sistemi esperti ai sistemi intelligenti.

I sistemi di intelligenza artificiale si distinguono: in *software based*, che adoperano programmi che operano solo nella realtà virtuale - si pensi ai sistemi di riconoscimento facciale oppure agli assistenti vocali - e sistemi incorporati in *hardware*, che incidono in modo diretto nella realtà delle cose, ad esempio, le automobili a guida autonoma e tutti i dispositivi riconducibili all'*Internet of things*.

Le ricerche basate su sistemi di IA possono condurre a due tipi di risultati: l'intelligenza specifica artificiale e l'intelligenza generale artificiale[84].

Nel primo caso la risposta della macchina sarà limitata allo scopo per il quale l'algoritmo era stato ideato quindi darà un risultato specifico; l'IA generale invece, dovrebbe condurre a soluzioni superiori a quelle raggiungibili da un soggetto umano.

L'orientamento scientifico prevalente ritiene che l'obiettivo di un'IA generale sarà presto raggiunto (nell'arco di qualche decennio) e sarà capace di realizzare il superamento di molti limiti dell'esistenza umana (come la

[84] Si veda: J. R. SEARLE, *"Minds, Brains and Programs"*, in *The Behavioural and Brain Science*, 1980, 417 ss.

malattia e l'invecchiamento) sebbene comporterà l'insorgere di nuovi rischi che dovranno essere presto affrontati e superati[85].

Un'altra distinzione, degna di nota, è quella tra IA *debole*[86] e IA *forte*: la prima sviluppa sistemi capaci di simulare i comportamenti umani, ma non di pensare e riprodurre gli stessi processi mentre l'IA *forte* è letteralmente capace di pensare e capire, questo naturalmente rappresenta un notevole passo avanti, ma allo stesso tempo è fonte di rischi e pone numerosi punti interrogativi.

L'idea di sviluppare un'intelligenza artificiale *forte* inizia a prendere forma a partire dal contributo di Alan Turing[87] che si domandava se fosse possibile creare macchine intelligenti, per poi verificare successivamente i risultati raggiunti.

Come anticipato, lo studioso ideò un *test* che prende il suo nome e si ispira ad un gioco di società nel quale vengono interrogati da una terza persona due interlocutori (di sesso diverso) al fine di indovinare chi sia l'uomo e chi la donna a seconda delle risposte fornite.

In breve, il gioco c.d. dell'imitazione coinvolge tre persone un uomo, una donna e un interrogante. Lo scopo del gioco è consentire all'interrogante di capire chi sia l'uomo e chi la donna. I tre soggetti si trovano in tre stanze diverse e tramite dialoghi che si basano su quesiti-risposte l'interrogante

[85] A. M. TURING, *Computer Machinery and Intelligence*, cit., 433 ss.
[86] S. J. RUSSEL-P. NORVING, *Artificial Intelligence – A modern approach*, 2010, 1020 ss.
[87] Sul punto si rinvia a: A. M. TURING, *Computer Machinery and Intelligence*, cit., 433 ss.

stabilirà il sesso di A e B. Se si sostituisse A con una macchina l'interrogante sarebbe capace di comprendere che a rispondere non è stato un essere umano, ma l'intelligenza artificiale?

I risultati ottenuti non hanno ancora dato un esito positivo; quindi, nessuna macchina ha superato il *test*; da ciò, ne deriva che l'IA è lontana da una completa uguaglianza con l'intelligenza umana nell'interlocuzione verbale, ma ciò non esclude che in un prossimo futuro tale obiettivo potrebbe essere raggiunto.

Gli strumenti dell'IA sono alimentati dai dati - nello specifico da *Big Data* – ossia da informazioni che vengono processate e correlate tra loro da algoritmi che sono i veri motori logici dell'intelligenza artificiale.

In realtà, le tecniche di apprendimento sono molteplici; infatti, si parte da strumenti c.d. *logic e knowledge based* fino ad arrivare al *machine learning*[88]. Queste ultime sono considerate le più avanzate, in quanto si basano sull'autoapprendimento e partendo da un determinato *input* sono capaci di perfezionare la loro *performance* raggiungendo un risultato che non è determinabile a priori dall'ideatore.

I dispositivi basati sul *machine learning* devono perseguire un determinato obiettivo, ma nel corso del tempo possono imparare a raggiungerlo in maniera

[88] Si veda: B. P. GOECKE, *Artificial Intelligence*, Padeborn, 2020; P. WANG, *On Defining Artificial Intelligence*, in *Journal of Artificial Intelligence*, 10, 2017, 1; M. A. BOEDEN, *Artificial Intelligence. A Very Short introduction*, Oxford, 2018.

sempre più efficiente. Questa tecnica rappresenta il superamento della tecnologia tradizionale fondata su un funzionamento logico-deduttivo.

Generalmente, la macchina svolgeva il proprio compito in base ad una tecnica predeterminata e quindi il risultato cui perveniva era sempre prevedibile; in caso di *machine learning,* il sistema è dotato di apprendimento automatico pertanto analizza i dati, li elabora ed "impara" dagli stessi, dando un risultato non standardizzabile.

Sia che si tratti di sistemi c.d. esperti - basati su un funzionamento logico-deduttivo - che di macchine capaci di auto-apprendere la fase più importante è il *training*[89].

L'algoritmo - che possiamo definire il motore dell'intelligenza artificiale - viene allenato dall'ideatore ad analizzare e riconoscere i criteri in base ai quali classificare le informazioni.

Si parla di *supervised learning* quando l'algoritmo processa un'enorme mole di esempi, dotati di un'etichetta, con l'obiettivo di sviluppare la capacità di riconoscimento e classificazione degli *input* iniziali.

Esistono tecniche più avanzate di *training* algoritmico si tratta del *reinforcement learning* e del *unsupervised learning*.

[89] Per un approfondimento sulle varie tipologie di *training* si veda: N. ABRIANI, G. SCHNEIDER, *Diritto delle imprese e intelligenza artificiale. Dalla Fintech alla Corptech*, Bologna, 2021.

Il *reinforcement learning*, o per rinforzo, non si basa su una serie di istruzioni predefinite, ma l'agente di apprendimento viene preparato per rinforzo utilizzando un sistema di premi e penalità.

In altre parole, il processo contiene la definizione e simulazione dell'ambiente in cui opera l'agente, il segnale di ricompensa, la *polic*y dell'algoritmo ed il funzionamento di quest'ultima.

L'agente non conosce a priori come compiere determinate azioni e come raggiungere il risultato, ma sa solo quale è l'obiettivo che dovrà raggiungere basandosi sull'esperienza e procedendo per tentativi.

Nel caso in cui raggiungerà il risultato sperato avrà una ricompensa in caso contrario una penalità.

Questa tecnica è molto simile all'apprendimento umano in quanto riproduce la capacità di imparare dall'esperienza e di reagire a situazioni nuove ed imprevedibili apriori, però è un modo di procedere molto complesso e non si adatta facilmente a tutti i tipi di funzioni.

L'*unsupervised learning* invece, non procede per tentativi, ma gli algoritmi vengono sviluppati per individuare i propri criteri dai dati di carattere non strutturato che i sistemi raccolgono dall'ambiente in cui operano.

I sistemi esperti sono riconducibili a tecniche di *machine learning* che rendono la macchina capace di elaborare autonomamente i dati immessi senza seguire dei criteri predeterminati.

La correttezza del risultato dipenderà dal numero di informazioni e di esempi forniti che daranno modo all'algoritmo di sviluppare soluzioni sempre più avanzate.

Orbene, l'apprendimento automatico si basa su reti neurali artificiali che, come suggerisce il nome, mirano a riprodurre quanto avviene nel cervello umano.

Le reti neurali possono avere una complessità variabile, quelle più sofisticate hanno una struttura multilivello (*deep learning networks*) molto simile al cervello umano.

Quindi dal tipo di *training* che viene impiegato e dalla complessità dell'algoritmo dipende il grado di indipendenza della macchina e di conseguenza la sostituibilità all'essere umano.

Complementare a questo aspetto è il tipo di relazione che si crea tra l'intelligenza artificiale e quella umana; ad esempio, si parla di intelligenza assistita quando l'utilizzatore mantiene il pieno controllo sulle decisioni adottate dalla macchina.

Il grado di autonomia dell'algoritmo nell'elaborare risposte raggiunge l'apice in caso di intelligenza autonoma – l'esempio classico sono le *self-driving cars* – dove la macchina può sostituirsi all'uomo e non necessita di *input* continui per operare.

Il passaggio dall'automazione tecnologica all'autonomia digitale rappresenta il vero "costo-beneficio" dell'intelligenza artificiale, in quanto la capacità di

elaborare un sistema decisionale autonomo[90] rispetto alle indicazioni impartite, costituisce una forma di progresso, ma è anche fonte di problemi giuridici che occupano gli operatori del diritto fin dalla fine del XIX secolo.

Gli interrogativi che suscitano le nuove forme di intelligenza artificiale sono molteplici, ma due sono le principali problematiche e riguardano: la qualificazione giuridica dei sistemi di IA e la responsabilità configurabile in caso di offesa a beni giuridici rilevanti, perpetrata dagli agenti artificiali.

Il dibattito sull'opportunità di riconoscere la personalità giuridica[91] a tali sistemi è ancora aperto e si può dire che due siano le posizioni contrapposte: la prima, ritiene che attribuire la personalità giuridica ad un'entità artificiale sarebbe pericoloso, soprattutto da un punto di vista etico; mentre la seconda – ad oggi minoritaria – è favorevole a detto riconoscimento.

Una parte della dottrina ipotizza di estendere all'IA la soggettività giuridica ripercorrendo il processo che ha portato al riconoscimento di tale attributo ad enti e persone giuridiche. Tuttavia, un tale parallelismo non sembrerebbe ipotizzabile in quanto la persona giuridica coincide con un insieme di persone che agiscono in virtù di un rapporto di immedesimazione organica e tale attributo non è riferibile anche alla macchina.

---

[90] Alcuni autori parlano di comportamento emergente in quanto ritengono che il termine autonomo associato alle decisioni della macchina lasci trasparire una sorta di intenzionalità. Si veda: R. CALÒ, *Robotics and the Lesson of Cyberlaw*, in *California Law Rewiew*, 2016, 103, 538 ss.; T. C. KING, N. AGGRARWAL, M. TADDEO, L. FLORIDI, *Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions*, in *Science and Engineering Ethics*, 2020, 26, 94 ss.

[91] Sulla contrapposizione tra le due tesi si veda: N. NAFFINE, *Who are Law's Persons? From Cheshire Cats to Responsabile Subjects*, in *Modern law Review*, 2003, 1, 346 ss.

La persona giuridica costituisce una vera e propria *fictio iuris* realizzata per attribuire al gruppo le responsabilità per azioni poste in essere nell'interesse della società; nel caso dell'IA si tratta di un agente che ha un corpo fisico o digitale, ma che rimane distinto dal soggetto che lo ha ideato o utilizzato.

Pertanto, bisognerebbe ragionare sul legame che si instaura tra persona fisica ed agente artificiale più che attribuire a quest'ultimo una personalità giuridica.

La responsabilizzazione in via esclusiva della macchina comporterebbe un'eccessiva deresponsabilizzazione di coloro che entrano in contatto con la stessa dal momento dell'ideazione.

Il secondo problema - connesso all'inopportunità allo stato degli atti di riconoscere la personalità giuridica all'agente artificiale - riguarda l'imputazione delle azioni e dei reati commessi per il tramite dell'agente artificiale o direttamente da quest'ultimo (tale tema verrà approfondito nei prossimi paragrafi).

Lo sviluppo della tecnologia porta con sé nuove forme di reati e determina la nascita di nuovi metodi criminosi[92].

[92] Al riguardo si parla di diritto penale dell'IA che sta assumendo un rapido sviluppo in plurimi campi di indagine; a titolo esemplificativo si veda: l'esperimento degli scienziati Seymor e Tully che usarono la tecnologia per convincere gli utenti a cliccare su *links* di *phishing* (J. SEMYOR, P. TULLY, *Weaponizing Data Science for Social Engineering: Automated E2E Spear Phishing on Twitter*, 2016); ai plurimi incidenti stradali realizzati negli Stati Uniti dalle auto a guida autonoma; ai messaggi d'odio diffusi da *social bots*, come nel caso del *social bot* di Twitter "Tay" che ha appeso dalle interazioni degli utenti ed ha iniziato ad inviare messaggi con contenuto provocatorio ad esponenti di un movimento femminista (si veda G. NEFF, P. NAGY, *Talking to Bots: Symbiotic Agency and the Case of Tay, in International Journal of Communication*, 2016, 10, 4915; M. LAMO, R. CALO, *Regulating Bot Speech*, in U.C.L.A. *Law Rewiew*, 2019, 988, 66.

La questione investe plurimi settori del diritto penale, ma si può dire che i reati che hanno subito un "mutamento" sono: i reati in materia di mercati finanziari, i reati informatici, il traffico di stupefacenti o altri prodotti illeciti e i reati contro la persona, intesa in senso lato.

Il tema è stato affrontato anche in ambito civilistico[93] dove, in primo luogo, si è cercato di stabilire se l'attribuzione della capacità giuridica sia il presupposto per l'individuazione della disciplina applicabile oppure sia una mera formula per descrivere una posizione giuridica ricostruita mediante un percorso diverso.

Secondo alcuni autori il problema della capacità giuridica degli agenti artificiali si tramuta nella possibilità di applicare agli stessi la normativa prevista per le persone fisiche.

A tal proposito, sono state elaborate tre diverse teorie: organica, costituzionale e atomistica.

La prima presuppone che la capacità giuridica venga attribuita dal legislatore, quindi, non sussista alcun tipo di identità tra l'uomo ed il soggetto di diritto[94]. L'uomo, in base alla teoria organica diviene soggetto di diritto solo per effetto della disposizione normativa.

---

[93] A. AZARA, *Intelligenza artificiale e personalità giuridica*, in *Il diritto nell'era digitale*, a cura di R. GIORDANO, A. PANZAROLA, A. POLICE, S. PREZIOSI, M. PROTO, Milano, 2022, 91 ss.

[94] P. RESCIGNO, *voce Capacità giuridica*, in *Dig. Disc. Priv*. (sez. civ.), II, Torino, 1988, 218 ss.; U. RUFFOLO, *Il problema della personalità elettronica*, in U. RUFFOLO (a cura di), *L'intelligenza artificiale – Il diritto, i diritti, l'etica*, Milano 2020, 217.

La teoria costituzionale[95] ritiene che la capacità giuridica sia un attributo della sola persona fisica e quindi preclude a priori qualunque tipo di interpretazione analogica con l'agente artificiale.

Infine, la teoria atomistica rifiuta l'identificazione della capacità giuridica con il soggetto umano, ma ammette un'interpretazione che muova da un controllo di compatibilità e congruità con gli interessi coinvolti[96].

In base alla concezione atomistica, non esiste una logica binaria oggetto-soggetto, ma l'agente *software* sarà qualificabile come un soggetto di diritto quando utilizzando il ragionamento che si basa sull'analogia, le norme che si riferiscono all'agente umano siano riferibili anche alla macchina.

L'interprete valuterà in primo luogo le norme applicabili e successivamente indicherà la disciplina individuata alla luce del concetto di capacità giuridica.

La prevalente dottrina[97] ritiene che quest'ultima sia l'unica teoria che si attaglia alla complessità della disciplina; in quanto non tenta di costruire un modello basandosi sulla mera identificazione oggetto-soggetto, ma parte dalle funzioni che caratterizzano l'agente artificiale per capire quale sia la disciplina applicabile e per trovare la conseguente soluzione giuridica.

La complessità del sistema rende necessario un approfondimento che verrà sviluppato nei prossimi paragrafi; in ogni caso, si può constatare che il

---

[95] P. STANZIONE, *Capacità e minore età nella problematica della persona umana*, Camerino-Napoli, 1975; ID, *Capacità* (diritto privato), in *Enc. Giur.*, V, Roma, 1988, 6 ss.

[96] G. PERLINGIERI, *Profili applicativi della ragionevolezza nel diritto civile*, Napoli, 2015; L. VIZZONI, *Domotica e diritto. La Smart Home tra regole e responsabilità*, Milano, 2021, 35-36.

[97] Tra gli altri: A. AZARA, *Intelligenza artificiale e personalità giuridica*, cit., 103 ss.

passaggio da sistemi esperti a sistemi intelligenti dipende in massima parte dal tipo di dati inseriti e questo dimostra come al centro dell'indagine debbano essere sempre posti i c.d. *data*.

1.2 La base della ricerca algoritmica. I *Big Data*.

L'intelligenza artificiale può operare perché uno specifico algoritmo viene impostato per consentirle di svolgere determinate operazioni.

Le tecnologie più avanzate non solo sono capaci di elaborare le informazioni, ma di autoapprendere realizzando dei risultati che non sono completamente prevedibili da parte di colui che ha progettato la macchina oppure dall'utilizzatore.

La ricerca algoritmica, si alimenta grazie ai dati o meglio ai c.d. *Big Data*.

Questi ultimi sono delle grandi masse di informazioni catalogate e selezionate che consentono di effettuare delle ricerche e delle operazioni su larga scala[98].

Sebbene si faccia riferimento ai dati è necessario chiarire che non si tratta di dati personali, ma di riferimenti pseudonimizzati o inferiti, in altre parole non sono riferibili direttamente alla persona di cui si tratta, se non utilizzando delle informazioni aggiuntive.

[98] Per una dettagliata definizione si veda: G. SARTOR, *L'intelligenza artificiale e il diritto*, cit., l'Autore fa riferimento alle caratteristiche principali dei *big data* ossia le tre V: enorme Volume, alta Velocità e grande Varietà. Inoltre, sottolinea che spesso vengono associati ai dati massivi la bassa Veracità (che comporta spesso l'inaccuratezza delle informazioni) e l'alto Valore (l'utilità, correlata all'ampiezza della massa).

In realtà, questo è vero solo in parte in quanto i *big data*, anche se non contengono delle informazioni personali, possono essere ricondotti ad un soggetto determinato adoperando uno specifico algoritmo.

L'origine dei dati massivi può essere umana ed analitica, ma molto spesso avviene in forma automatizzata, in quanto gli stessi vengono estrapolati da dispositivi che catalogano le informazioni del mondo fisico.

In ogni caso, i dati costituiscono una fonte di estremo rilievo sia per le aziende che per i governi in quanto vengono utilizzati per adoperare strategie di *marketing*, ma anche per orientare le decisioni.

La caratteristica principale dei dati massivi è connessa al loro utilizzo per finalità analitica; tale funzionalità consente di collegare tra loro i dati e di fare predizioni.

I *big data* sono sicuramente una fonte ineludibile nella c.d. *New economy*, ma determinano una serie di rischi; tra questi emergono le difficoltà di conciliare la raccolta e l'utilizzo di tali masse di dati con la tutela della *privacy* e degli altri interessi coinvolti.

1.3 I reati commessi tramite i sistemi di IA.

In ambito penale, l'intelligenza artificiale può assumere una diversa funzione in quanto può rappresentare sia il mezzo che l'autore del reato.

La macchina potrebbe essere progettata al fine di commettere dei reati e quindi essere il mezzo di esecuzione.

Da questo punto di vista le fattispecie che possono essere realizzate tramite i sistemi intelligenti sono plurime; si pensi all'utilizzo dell'IA per commettere reati informatici[99], diffondere materiali senza il consenso del soggetto interessato, ma anche ai casi in cui ad essere ingannati siano gli stessi sistemi artificiali: ciò può avvenire ad esempio, nelle macchine a guida autonoma che vengono impostate in modo da non rilevare un limite di velocità oppure nel caso degli assistenti vocali utilizzati per accedere a siti *web* illeciti o digitare numeri telefonici[100].

Questi sono solo alcuni esempi, ma il vero problema è l'adeguamento delle fattispecie esistenti alle nuove forme di realizzazione dei reati; si pensi al caso in cui ad essere ingannata sia una macchina artificiale, potrebbe trattarsi di *hacking*[101]?

Orbene, è presumibile che - come tutte le fasi di "transizione" - il compito di risolvere i dubbi ermeneutici verrà affidato all'interprete che cercherà di adeguare la normativa esistente alle nuove tecnologie.

---

[99] R. ABBOTT, A. SARCH, *Punishing Artificial intelligence: Legal Fiction or Science Fiction*, in *UC Davis Law Review*, 2019, 53, 330 ss.

[100] K. J. HAYWARD, M. M. MAAS, *Artificial Intelligence and crime: A primer for criminologist*, in *Crime Media Culture*, 2020, 7 ss.; B. PANATTONI, *Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'autonomia digitale*, cit., 9.

[101] Sul punto si veda: R. CALÒ, I. EVTIMOV, E. FERNANDS ET AL., *Is Tricking a Robot Hacking?*, in *Berkeley Technology Law Journal*, 2019, 34, 891 ss.; S. S. BEALE, P. BERRIS, *Hacking the Internet of Things: Vulnerabilities, Dangers, and Legal Responses*, in *Duke Law & Technology Review*, 2017-2018, 16, 161 ss.

1.3.1 L'algoritmo come autore del reato.

Il secondo problema che emerge dallo sviluppo dell'IA – nello specifico di sistemi intelligenti capaci di auto-apprendere e di realizzare dei risultati non prevedibili anticipatamente – riguarda l'imputazione dell'illecito commesso dalla macchina.

Il tema è all'attenzione dell'Unione Europea che con l'*AI Act*[102] si propone di sviluppare una regolazione che riesca a governare i diversi rischi che connotano l'intelligenza artificiale.

La prima questione che è necessario affrontare riguarda il rischio che il sistema artificiale cagioni delle offese a beni giuridici facenti capo ad utenti o terzi che entrano in contatto con esso[103].

Invero, si deve considerare che le macchine – come detto – sono capaci di produrre dei risultati non prevedibili *ex ante* e quindi si può dire che abbiano capacità decisionale. Si pensi al caso emblematico del c. d. *Random Darknet shopper*, un algoritmo programmato per acquistare, ogni settimana in modo casuale dal *Deep web* degli oggetti da esporre ad una mostra di Zurigo.

In quel caso l'agente artificiale acquistò delle droghe illegali e quindi commise un illecito penale ai sensi del diritto svizzero[104].

---

[102] Il 14 giugno 2023 il Parlamento Europeo ha approvato *l'Artificial Intelligence Act* (*AI Act*).

[103] R. CALO, *Robotics and the Lesson of cyberlaw*, cit.

[104] F. LAGIOIA, G. SARTOR, *AI system under Criminal Law: a Legal Analysis and a Regulotary Perspective*, in *Philosophy Tecnology*, 2019, 1 ss.

In tal caso il vero interrogativo riguarda il tipo di rimprovero che può essere mosso nei confronti del programmatore oppure dell'utilizzatore; sul punto si constata che l'orientamento prevalente imputa all'operatore una responsabilità per mancato impedimento colposo.

L'IA autonoma supera il principio secondo il quale la tecnologia può rappresentare solo uno strumento, in quanto l'agente umano quando utilizzerà sistemi intelligenti si troverà a dover vigilare sulla correttezza delle decisioni prese da questi ultimi oppure a fondare i propri comportamenti su presupposti completamente delineati dalla macchina[105].

Gli operatori si trovano a fronteggiare il c.d. "*control dilemma*"[106], dove si configura essenzialmente un problema di controllo; infatti, se da un lato l'agente artificiale garantisce in astratto prestazioni più performanti in termini di precisone, analiticità e rapidità della decisione, dall'altro relega l'operatore a semplice controllore.

Spesso però, la vigilanza e l'analisi dell'operato dell'agente artificiale viene ostacolato dalle stesse caratteristiche della tecnologia. Le difficoltà cui va incontro l'operatore sono dettate in primo luogo, dalle elevate capacità computazionali delle macchine che non gli consentono di effettuare un controllo contestuale; in secondo luogo, dal rischio che l'attenzione possa

[105] A. SIMONCINI, S. SUWEIS, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto costituzionale*, in *Riv. fil. Dir*., 2019, 1, 93 ss.

[106] E. HIGENDOLRF, *Automated Driving and the Law*, Baden-Baden, 2017, 181 ss.; J. ZERILLI, A. KNOTT, J. MACLAURIN, C. GAVAGHAN, *Algoritmic Decision-Making and the Control Problem*, in *Minds and Machines*, 2019, 29, 555 ss.; A. CAPELLINI, *Profili penalistici delle self-driving cars*, in *Dir. Pen. Cont*., 2019, 2, 335 ss.

venire meno durante il monitoraggio ed infine, dalla fiducia che spesso si ripone negli agenti artificiali e nei risultati che producono.

Alla luce di queste considerazioni si può dire che allo stato degli atti è complesso costruire un regime di imputazione in capo all'operatore[107] non solo per la forte autonomia che caratterizza le nuove forme di intelligenza artificiale, ma anche per l'opacità[108] (che si tratterà approfonditamente nei prossimi paragrafi) dei sistemi e la molteplicità dei soggetti[109] che vengono in contatto con la macchina nel corso del suo funzionamento.

Quindi, se da un lato l'algoritmo può essere materialmente autore del reato, il mancato riconoscimento di un'autonoma personalità giuridica, pone il problema di delineare la responsabilità degli operatori che si rapportano con il sistema artificiale.

Nello specifico tali soggetti sono: il produttore, il progettista, l'addestratore, coloro che collezionano i dati, i venditori, gli acquirenti ed infine, l'utilizzatore.

---

[107] R. ABBOT, A. SARCH, *Punishing Artificial Intelligence: Legal Fiction or Science Fiction*, in *UC Davis Law Review*, 2019, 53, 355 ss.; gli Autori ritengono che sono plurimi i motivi che non consentono di ricondurre i reati commessi dall'IA ad un agente umano: (i) problemi di *enforcement,* in quanto spesso l'agente che ha programmato il sistema ha la possibilità di rimanere anonimo, (ii) la pluralità di agenti rende difficile isolare il contributo del singolo; (iii) problemi di *policy*, in quanto ritenere tutti gli operatori responsabili può essere considerata una politica criminale scorretta.

[108] J. BURREL, *How the machine "thinks": Understanding opacity in machine learning algorithms*, in *Big Data & Society*, 2016, n. 3, 1 ss.

[109] F. BASILE, *Intelligenza artificiale e diritto penale: quattro possibili percorsi d'indagine*, in *Diritto Penale e Uomo*, 29 settembre 2019, 27 ss.; M. B. MAGRO, *Decisione umana e decisone robotica. Un'ipotesi di responsabilità da decisone robotica*, in *La Legislazione penale*, 10 maggio 2020, 3 ss.

Il diverso grado di autonomia della macchina si riverbera sul tipo di responsabilità riconducibile all'agente umano – commissiva o omissiva – e sul soggetto della catena cui tale rimprovero può essere mosso. Si può notare come la maggiore autonomia dell'algoritmo sposta l'indagine dal fruitore ai soggetti che si collocano prima nella "catena" di utilizzo.

Orbene, si comprende come il tema sia complesso e necessiti di un approfondimento partendo dalle basi ed analizzando in primo luogo la tecnologia di riferimento, per questo motivo nei prossimi paragrafi oggetto d'indagine saranno proprio le varie forme di tecnologia emergenti – senza pretesa di esaustività – e le loro caratteristiche.

2. Le caratteristiche della *Blockchain*.

La *blockchain* rappresenta una *species* del *genus* intelligenza artificiale.

Si basa su algoritmi e reti informatiche però, si differenzia dall'IA in quanto non si basa sui c.d. *big data* e non realizza delle analisi statistiche e predittive, ma si "poggia" su una catena di blocchi concatenati che consente il trasferimento di informazioni crittografate.

La *blockchain* è una tecnologia basata sulle c.d. *distribuited ledger technologies*, nello specifico ne costituisce una *species*.

I dati inseriti tramite crittografia asimmetrica, sono allocati in blocchi, accompagnati da *hash* e validazione temporale, tra loro concatenati attraverso

il richiamo dell'*hash* precedente in quello successivo, garantendone l'immodificabilità unilaterale[110].

Ogni nuovo blocco è validato da alcuni nodi (detti *miners*) per mezzo della risoluzione di un problema matematico, che ne garantisce la corretta validazione.

La *blockchain* può essere assimilata ad un registro o ad un libro mastro digitale, che conserva in modo immutabile la memoria storica delle transazioni avvenute ed in cui in modo paritetico, ciascun partecipante dispone di una copia della singola operazione garantendone la sicurezza e resistenza rispetto a potenziali attacchi.

Le caratteristiche delle tecnologie a registro distribuito possono essere riassunte in: disintermediazione, decentralizzazione, distribuzione e vocazione transnazionale, immutabilità, inalterabilità e persistenza dei dati, consenso distribuito, trasparenza e tracciabilità.

L'ideatore della *blockchain* viene identificato con Satoshi Nakamoto – pseudonimo di un autore la cui identità risulta sconosciuta – il quale mise appunto il registro che avrebbe dovuto tenere traccia di tutte le transazioni di *bitcoin*.

Il sistema però, ben presto trovò largo uso anche in altri ambiti proprio per la sicurezza e la trasparenza che lo contraddistingue.

[110] A. PERNA, *Le origini della blockchain*, in *Blockchain e smart contract*, Milano, 2019,

Uno degli obiettivi più importanti delle tecnologie a registro distribuito è il superamento del sistema centralizzato di validazione. Le DLT in generale e la *blockchain* in particolare utilizzano un sistema di crittografia che prevede un meccanismo di firma a doppia chiave asimmetrica per cui l'utente entra in possesso di una chiave pubblica ed una privata che gli consentono di effettuare transazioni oppure aprire *smart contract* o altri servizi.

Alla base della validazione delle transazioni vi è il consenso che deve essere fornito da ogni nodo della catena[111].

Il blocco una volta inserito non è più modificabile, o meglio astrattamente potrà subire delle modifiche, ma queste dovranno essere validate da tutti i nodi della catena.

Il sistema come si vedrà approfonditamente nei prossimi paragrafi è particolarmente sicuro proprio per le caratteristiche che lo contraddistinguono.

Sebbene il settore trainante in cui la *blockchain* ha avuto maggiore applicazione è quello finanziario, quest'ultima si sta diffondendo su vari livelli.

Si pensi al settore della *supply chain* e della logistica, dove grazie a questo meccanismo è possibile seguire il prodotto lungo tutta la catena di approvvigionamento e commercializzazione; oppure, al settore sanitario dove

[111] Per un approfondimento sul funzionamento della *blockchain* e sulle tecnologie che sono alla base della stessa si veda, *ex multis*: D. CARBONI, *Le tecnologie alla base della blockchain*, in *Blockchain e smart contract*, Milano, 2019, 33 ss.

i dati immagazzinati possono essere condivisi e tracciati in sicurezza consentendo una collaborazione più efficace ed un miglioramento del servizio e della ricerca.

Un altro settore in cui è possibile utilizzare la *blockchain* è quello degli appalti, dove l'immodificabilità e la trasparenza dei dati e delle certificazioni consente, non di escludere, ma quantomeno di prevenire il rischio corruzione.

2.1 Le tecnologie a registro distribuito.

La prima definizione di tecnologie a registro distribuito nel nostro ordinamento si rinviene all'articolo 8-ter del decreto-legge n. 135 del 2018 (c.d. decreto Semplificazioni), convertito in legge 12/2018[112].

La rubrica dell'articolo fa riferimento alle tecnologie basate su registri distribuiti e *smart contract* mentre la norma disciplina questa nuova forma di registro distribuito volto a facilitare le transazioni e la sicurezza delle stesse, che è favorita da una immodificabilità dei dati presenti all'interno del registro.

L'articolo 8-ter del d.l. 135/2018 stabilisce che: "*1. Si definiscono «tecnologie basate su registri distribuiti» le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e*

[112]M. SIMBULA, *La normativa italiana sulle DLT*, in *Blockchain e smart contract*, Milano, 2019, 135 ss.

l'archiviazione sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante non alterabili e non modificabili".

La dottrina di fronte alla definizione delle tecnologie a registro distribuito ha presentato plurime perplessità, a partire dalla definizione di "basi crittografiche" che siano "architetturalmente decentralizzate".

Prendendo in considerazione il registro, ad esempio, quello basato sui Bitcoin[113], si può notare come i dati in esso contenuto siano replicati in ogni nodo della rete; pertanto, ogni nodo contiene la totalità dei dati.

Quindi, sebbene la norma faccia rifermento alla decentralizzazione del registro sembrerebbe più opportuno riferirlo all'accesso allo stesso. Un'altra criticità, si può riscontrare nel riferimento all'immodificabilità dei dati inseriti nel registro. Questa caratteristica sussiste in astratto, ma in concreto qualora vi fosse il consenso di tutti coloro che appartengono alla rete tale modifica potrebbe essere operata.

Sicuramente, sussistono delle difficoltà interpretative dovute anche all'ambiguità della normativa di riferimento, ma non si può non considerare che tale tecnologia ha plurimi vantaggi.

Il tipo di DLT più diffuso è senza dubbio la *blockchain* che viene definita come un registro replicabile e verificabile, che garantisce una forte integrità tramite l'utilizzo di funzioni crittografiche e il cui accesso è centralizzato ed

[113] Si veda: S. NAKAMOTO, *Bitcoin: A Peer-to-Peer Eletronic Cash System*, in https://bitcoin.com

è disciplinato da un protocollo che permette la scrittura di nuovi elementi solo qualora sussista l'accordo dei soggetti appartenenti alla rete.

Il requisito dell'immodificabilità – come anticipato – deve essere correttamente contestualizzato perché in astratto il sistema diventa suscettibile di modifiche a fronte del consenso di tutti i soggetti appartenenti alla catena. Questa caratteristica rende le DTL in generale e la *blockchain* in particolare, sicure ed utilizzabili per rivoluzionare plurimi settori come, ad esempio, quello finanziario.

2.2 Gli *Smart Contracts*. La validazione ed il valore probatorio dei documenti salvati in *blockchain*.

Una prima definizione di *smart contract* nell'ordinamento italiano si rinviene nello stesso articolo 8-ter, del d.l n. 135 del 2018, secondo cui "*si definisce smart contract un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola due o più parti sulla base di effetti predefiniti dalle stesse*"[114].

Gli *smart contract*, infatti, sono un programma per elaboratore che unisce il protocollo *blockchain* con il *software* sul quale lo stesso è "ospitato"[115].

[114] Si veda: R. BATTAGLINI, *La normativa italiana sugli smart contract*, in *Blockchain e smart contract*, Milano, 2019, 375.

[115] C. AMATO, *La computerizzazione del* contratto *(smart, data oriented, computable e self-drivingcontract. Una panoramica),* in *Eur. Dir. priv*., 2020, 1268.

Tale tipo di programma si esegue automaticamente, quindi una volta inserite le condizioni di funzionamento e realizzazione, si autoesegue e l'iniziativa non è più ricollegabile alle parti[116].

L'ideatore del *software* è stato lo scienziato, matematico, giurista e crittografo Nick Szabo che ebbe l'intuizione di unire la logica computazionale alla tradizione contrattualistica[117]; in questo modo, la logica computazionale si poneva al servizio di un processo volto alla risoluzione di un problema.

A partire dal 2008, grazie agli studi di Satoshi Nakamoto, nasce la *blockchain*, che consente la trascrizione di dati su registri distribuiti.

Nel 2013 viene "suggellata" l'unione tra *smart contract* e *blockchain*, con l'invenzione di *Ethereum*[118], il sistema interamente dedicato agli *smart contract*.

Quest'ultimo costruisce un *software* in cui, all'interno di una *blockchain* possono interagire i contratti *smart* che aveva teorizzato Sazabo. Lo studioso ungherese parlava di programmi computazionali che dovevano essere *smart* e *contract* facendo riferimento più al fine che alle loro caratteristiche. Infatti, questi potevano essere rappresentativi di accordi, ma non potevano essere impiegati comunemente. La *Ethereum* di Buterin[119], invece sviluppa un

---

[116] A. SAVELYEV, *Contract law 2.0: Smart'contracts as the beginning of the end of classic contract law*, in *Information & Communications Technology Law*, 2017, 122 ss.

[117] T. BELARDI, *Gli smart contract: storia e definizioni di un ibrido contratto/software*, in *Blokchain e smart contract*, Milano, 2019, 225 ss.

[118] T. BELARDI, *Gli smart contract: storia e definizioni di un ibrido contratto/software*, cit., 230 ss.

[119] V. BUTERIN, *A next generation smart contract and decentralized application platform*, Ethereum White Paper, disponibile online.

sistema che può essere giuridicamente parificato al contratto, inteso in senso lato.

Lo *smart contract* è un accordo[120] che deve soddisfare determinati requisiti perché possa essere assimilato ai contratti di cui all'articolo 1321 c.c.; quindi, dovranno essere presenti gli elementi essenziali ai sensi dell'articolo 1325 c.c. quali: la volontà delle parti, la causa, l'oggetto, la forma, quando risulta prescritta dalla legge a pena di nullità.

Tali sistemi se posizionati su una *blockchain*, garantiscono l'immutabilità del dato, la trasparenza, l'incorruttibilità e la sicurezza.

In particolare, l'immutabilità del dato – da intendersi sempre in concreto – consente di garantire che le attività gestite mediante la piattaforma non possano essere modificate in corso di esecuzione, né rimesse al libero arbitrio di una delle parti coinvolte.

Una volta validato, il contratto viene eseguito automaticamente dal sistema e diviene un "*permanent script*"; le transazioni vengono annotate definitivamente sulla *blockchain* in cui esso opera.

Gli *smart contract* sono particolarmente sicuri perché le operazioni vengono salvate in tutti i nodi della catena, pertanto, un attacco informatico effettuato su un singolo dispositivo sarebbe improduttivo di effetti perché l'accordo continuerebbe ad essere efficace fino a quando risulti operativo almeno un registro.

---

[120] M. RASKIN, *The Law and Legality of Smart Contracts*, in *Georgetown Law & Tech Review*, 1, 311.

Come si può constatare, se da una parte molti sono i vantaggi degli *smart contract* dall'altra l'utilizzo di questi ultimi comporta plurime criticità.

In primo luogo, emerge la difficile accessibilità delle piattaforme su cui sviluppano gli accordi senza l'ausilio di un programmatore.

L'elevato tecnicismo dei codici telematici rende necessaria l'assistenza di un programmatore impedendo in concreto una diffusione massiva dei sistemi[121].

Si deve considerare che il codice[122] sulla base del quale lo *smart contract* si fonda è essenziale, pertanto, un errore o una falla nel sistema o nell'utilizzo dello stesso si riverbera sull'accordo.

Le prestazioni ottengono un'automatica esecuzione, pertanto non sono suscettibili di interpretazione e di aggiornamento in corso d'opera[123].

Quindi, uno dei limiti dello *smart contract* è proprio questo: la scarsa conoscibilità dei codici di funzionamento[124], tale aspetto rende necessario uno studio ed un intervento al fine di favorire l'utilizzo massivo della tecnologia, sfruttandone le molteplici potenzialità.

3. L'IA ed il sistema penale.

[121] E. MIK, *Smart contracts: Terminology, technical limitations and real world complexity*, in *Law, Innovation & Technology*, 2017, 1 ss.; R. O'SHIELDS, *Smart Contracts: Legal Agreements for the Blockchain*, in *N.C. Banking Inst*. 177, 2017, 190.

[122] E. BATTELLI, *Diritto privato digitale*, Milano, 2022, 261 ss.; P. BOUCHER, *Come la tecnologia blockchain può cambiarci la vita*, trad. it., Bruxelles, 2017, 15 ss.

[123] L. PIATTI, *Dal codice civile al codice binario: blockchain e smart contracts*, in *Cyberspazio e diritto*, 2016, 337.

[124] M. F. CAMPAGNA, *Gli scambi attraverso algoritmi e il problema del linguaggio*, in *Rivistawe*b, 1, 2019, 3.

Il progresso tecnologico sta avanzando in ogni settore della nostra società ed in ogni ambito giuridico; il diritto penale è stato pensato e costruito sull'uomo e richiede una responsabilità personale e colpevole che tradizionalmente viene giudicata da uomini in quanto, il giudizio presuppone una capacità valutativa e discrezionale che - al momento - risulta assente nell'agente artificiale.

Nonostante si possa pensare che l'intelligenza artificiale sia completamente incompatibile con il sistema penale, di fronte allo sviluppo ed al repentino affermarsi della tecnologia anche questa branca del diritto viene coinvolta.

Il primo problema da affrontare riguarda l'attribuzione della responsabilità per azioni poste in essere o autonomamente dalla macchina oppure in parte dall'uomo ed in parte dall'IA[125].

Un altro interrogativo riguarda il possibile adattamento degli schemi di imputazione basati sulla responsabilità personale e colpevole oppure l'adozione di nozioni nuove come la colpa di programmazione o di automazione che coinvolgano in primo luogo i soggetti che hanno prodotto la macchina[126].

Poi, ci si chiede se gli algoritmi possano essere utilizzati per la prevenzione dei reati, nell'ambito del *law enforcement*, nelle strategie di *criminal*

[125] U. RUFFOLO, *Intelligenza artificiale, machine learning e responsabilità da algoritmo*, in *Giur. It.*, 7, 2019, 1689.

[126] Sullo schema della *product liability*, si veda: U. RUFFOLO, *Intelligenza artificiale, machine learning e responsabilità da algoritmo*, cit., 7, 2019, 1694, 1697; A. AMIDEI, *Intelligenza artificiale e product liability: sviluppi del diritto dell'Unione Europea*, in *Giur. It.*, 2019, 1715.

compliance a livello aziendale e nelle attività di *risk assestment* del processo penale per calcolare il tasso di pericolosità sociale oppure il rischio di recidiva[127].

In un primo momento, la tecnologia aveva prodotto solo *software* che per ogni operazione necessitavano dell'ausilio umano, pertanto, risultava applicabile il modello di responsabilità vicaria che chiamava a rispondere, del fatto di reato, il programmatore, il costruttore oppure l'utilizzatore, quantomeno a titolo di colpa per non aver previsto una simile evoluzione del sistema artificiale, ciò era possibile perché l'agente era un mero strumento nelle mani della persona fisica.

La creazione di macchine capaci di autoapprendere[128] e di imparare in base alla loro esperienza ha determinato l'inidoneità del meccanismo della responsabilità vicaria, in quanto l'agente umano non ha più il completo controllo sulla macchina.

In ogni caso, come osservato da parte della dottrina,[129] l'intelligenza artificiale, al pari del diritto penale, promette la protezione di beni giuridici fondamentali, solo che l'IA promette una fattualità tecnologica mentre il diritto penale fornisce garanzie controfattuali.

---

[127] P. SEVERINO, *Intelligenza artificiale e diritto penale*, Milano, 2020, 532.

[128] Sul punto: E. HIGENDORF, *Autonome Systeme, Künstliche Intelligenz und Roboter*, in AA. VV. (a cura di S. BARTON ET AL.), *Festschrift für Thomas Fisher*, C. H. BECK, 2018, 111 ss.

[129] C. BURCHARD, *L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società*, cit.

Gli obiettivi più sfidanti dell'IA rapportata al diritto penale riguardano la riduzione della criminalità e l'obiettività delle decisioni giudiziali. La riduzione di alcune forme di reato viene connessa all'uso di *Smart contract* oppure al *Predictive o Big Data Policing*: per quanto riguarda gli *Smart contract* – come si è visto – automatizzando l'esecuzione dell'accordo e spostando la fiducia interpersonale in quella riposta nella macchina.

L'algoritmo - in linea teorica - garantisce che i soggetti rispettino gli accordi presi in quanto sono consapevoli che un comportamento contrario verrebbe impedito allo stesso sistema intelligente; un meccanismo simile pervade il *Predictive o Big Data Policing*, in quanto a fronte della scarsità di risorse, lo Stato si affida a strumenti capaci di semplificare le procedure e di analizzare dati massivi.

La differenza fondamentale tra *Predictive* e *Big Data policy* consiste nella platea cui si rivolge perché il primo è indirizzato al soggetto pubblico mentre il secondo anche al cittadino; la società accetta un controllo basato sui dati e fortemente pervasivo in cambio di una maggiore tutela dal crimine[130].

Le decisioni adottate dall'IA molto spesso non sono spiegabili (come si vedrà, si pone un problema di *explainability*), ma ciononostante, sono accettate e

[130] P. J. BRANTINGHAM, *The Logic of Data Bias and Its Impact on Place-Based Predictive Policing*, in *Ohio State Journal of Criminal La*w, 2018, 473; K. BRENNAN-MARQUEZ, *Big Data policing and the Redistribution of Anxiety*, in *Ohio State Journal of Criminal Law*, 2018, 487.

preferite da alcuni autori[131], rispetto alle valutazioni umane in quanto, garantirebbero una maggiore obiettività e neutralità di giudizio.

Le promesse dell'IA in ambito giudiziario spostano l'attenzione dalla fiducia nelle persone verso quella nell'alta tecnologia. L'utilizzo dell'algoritmo dovrebbe garantire l'obiettività, la neutralità e la coerenza[132] nell'applicazione del diritto.

Di fronte alle promesse della tecnologia sono diversi gli atteggiamenti che possono essere adottati: il primo orientamento che si è sviluppato parte da una concezione liberale del diritto penale, improntata al fine ultimo di tutela della libertà; mentre il secondo orientamento sposa idee *welfaristiche*, volte alla tutela della sicurezza[133].

---

[131] S. E. HENDERSON, *A Few Criminal Justice Big Data Rules,* in *Ohio State Journal of Criminal Law*, 2018, 527.

[132] Sul punto negli Stati Uniti si è sviluppata ed affermata la tesi che la tecnologia possa essere decisiva sia nella fase di prognosi della pericolosità del soggetto sia nel caso di commisurazione della pena facendo leva su una valutazione algoritmica dei rischi; emblematico è il caso State v. Loomis, deciso dalla Corte Suprema del Wisconsin. Eric Loomis, era sospettato di essere stato l'autista di un *drive-by-shooting*, e dichiaratosi colpevole non si è opposto all'accusa che lo incriminava per aver guidato un veicolo in assenza di autorizzazione. L'accusato era stato già condannato più volte, ma l'utilizzo di COMPAS (*Correctional Offender Managment Profiling for Alternative Sanctions*) ha generato una condanna a sei anni di reclusione, in quanto il soggetto era stato reputato a rischio recidiva ed un pericolo per la società.
Loomis propone ricorso per violazione del giusto processo, lamentando l'impossibilità di conoscere il meccanismo operativo dell'algoritmo perché coperto da segreto industriale; l'assenza di una decisione individualizzata perché si basava solo su dati generalizzati e l'inammissibilità della decisione perché valutava anche il genere del soggetto.
Il ricorso viene respinto dalla Corte Suprema di Wisconsin e la motivazione fa leva sul fatto che l'individuo non deve godere di un "diritto di spiegazione" di fronte ad una previsione algoritmica del rischio dal momento che ha la possibilità di conoscere i suoi *input* ed ha sufficienti informazioni sugli output; State v. Loomis, 881 N.W.2d 749 (2016) 754 (USA).

[133] K. GÜNTHER, *Bedrothe individuelle Freihithen im aufgelärten Strafrecht – Welche Freiheiten?*, in *KJ*, 2016, 250; C. BURCHARD, *L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società,* cit., 17.

In entrambi i casi è necessario un intervento da parte del legislatore al fine di operare un corretto bilanciamento e valorizzare le promesse dell'intelligenza artificiale.

Ci si deve domandare se la perdita di libertà da parte della società sia adeguatamente giustificata "dall'acquisto" in termini di innovazione ed ancora, se la garanzia di maggiore sicurezza, certezza ed obiettività decisionale ed operativa bilanci la perdita di fiducia nella capacità deliberativa dell'essere umano.

Orbene, nel prosieguo dell'elaborato verranno analizzate le problematiche connesse all'uso delle nuove tecnologie soprattutto, in relazione all'utilizzo ed al rapporto con i dogmi del diritto penale, partendo dalla questione relativa all'imputazione delle azioni commesse dalla macchina.

3.1 L'imputazione della responsabilità per azioni della macchina.

Il passaggio dagli strumenti di informazione a quelli di intelligenza artificiale – come anticipato – ha comportato la necessità di attuare un cambio di paradigma in quanto lo strumento tecnologico non viene utilizzato al solo scopo informativo, ma risulta capace di adottare decisioni in maniera automatizzata.

Sembra fondamentale a questo punto considerare l'aspetto relativo all'assetto delle categorie giuridiche. In primo luogo, a venire in considerazione è –

prima ancora che il riconoscimento della personalità giuridica all'agente artificiale – la configurazione del nesso di causalità tra gli eventi[134].

Fondamentale è la distinzione tra mezzo e soggetto agente, in quanto il primo è un mero strumento utilizzato per realizzare una determinata condotta mentre il secondo ha capacità decisionale e pertanto, è l'autore dell'evento[135].

L'intelligenza artificiale determina che lo strumento tecnologico non sia più da considerare come mero mezzo per la realizzazione di un evento, ma possa essere la stessa IA in maniera autonoma a realizzare la condotta.

Il fenomeno può essere 'visto' con scetticismo, ma è ormai inarrestabile, ciò determina la necessità di trovare una quadra che consenta di interpretare o meglio ripensare gli schemi giuridici classici alla luce dell'innovazione in atto.

Un altro interrogativo che occupa gli interpreti riguarda la responsabilità; chi risponderà degli eventuali danni realizzati dalla macchina intelligente?

Fino a quando la tecnologia costituiva solo il mezzo per porre in essere la condotta, del reato realizzato avrebbe risposto il soggetto agente o meglio l'utilizzatore (cui può essere imputata la condotta sia a livello oggettivo che soggettivo), ma gli strumenti di *machine learning* sono capaci di

---

[134] C. PIERGALLINI, *Intelligenza artificiale: da 'mezzo' ad 'autore' del reato?*, in *Riv. Italiana di diritto e procedura penale,* 4, 2020, 8 ss.

[135] A. SIMONCINI, S. SUWEIS, *Il cambio di pardigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Riv. Fil. Dir.*, 2019, 1, 93 ss.; E. HILGENDORF, *Automated Driving and the Law*, in E. HILGENDORF, U. SEIDEL (a cura di), *The Law*, Baden-Baden, 2017, 181 ss.

autoapprendere e di decidere autonomamente pertanto si pone il problema di comprendere chi è il responsabile ed a che titolo[136].

La prima forma di responsabilità che viene ipotizzata è quella per danno da prodotto[137].

Innanzitutto, è necessario chiarire che con riferimento all'agente artificiale i concetti di prodotto e produttore[138] vanno adeguatamente interpretati.

Infatti, il termine prodotto non si riferisce esclusivamente un artefatto robotico, ma anche alle applicazioni immateriali (i *software*) dell'IA; mentre il produttore comprende anche il programmatore e coloro che definiscono le caratteristiche della tecnologia e forniscono sostegno di *back-end*[139].

Il vero problema di fronte ad agenti intelligenti che autoapprendono e sono capaci di prendere decisioni in autonomia è che non è sempre possibile di parlare di difetto; in altre parole, non è detto che il danno sia il risultato di una difettosità dell'algoritmo applicato o della costruzione del prodotto[140]. In questo caso *quid iuris*?

Come si può arginare il *responsibility gap*?

---

[136] D. C. VALADECK, *Machine without principals: liability rules and Artificial*, in *Waschington Law Review*, 2014, 89, 150.

[137] A. AMIDEI, *Intelligenza artificiale e product liability: sviluppi del diritto dell'Unione Europea*, in *Giur. It.*, 2019, 7, 1715 ss.

[138] A. BERTOLINI, *Robot as Products: The case for a realistic analysis of robotic applications and liability rules*, in *Law Innovation and Technology*, 2013, 5,3, 214 ss.

[139] A. BERTOLINI, *Robot as a Products: the case for a realistic analysis of robotic applications and liability rules*, in *Law Innovation and Tecnology*, cit., 214 ss.

[140] A. AMIDEI, *Intelligenza artificiale e product liability: sviluppi del diritto dell'Unione Europea*, cit., 1715 ss.; U. RUFFOLO, *Per i fondamenti di un diritto della robotica self-learning, dalla machinery produttiva all'auto driverless: verso una responsabilità dell'algoritmo?*, in U. RUFFOLO (a cura di), *Intelligenza artificiale e responsabilità*, Milano, 2017, 13 ss.

La macchina, infatti, pone in essere comportamenti soggettivamente e oggettivamente imprevedibili. È progettata per realizzare un *outcome* non prevedibile e quindi l'eventuale reato posto in essere è frutto di tale progettazione, ma chi ne dovrà rispondere in concreto?

3.1.1 L'ipotesi di una responsabilità diretta dell'agente artificiale.

Gli agenti artificiali dotati di capacità di autoapprendimento in astratto – alla luce delle suesposte considerazioni – potrebbero porre in essere una condotta illecita, a tal proposito, ci si chiede se questa possa essere imputata alla stessa IA.

Una parte della dottrina - sebbene sia rimasta minoritaria - ha ipotizzato una responsabilità diretta a carico della macchina[141].

Tuttavia, tale ipotesi rimane ad uno stadio teorico, in quanto l'IA agisce sulla base di un algoritmo ed è capace, in base all'esperienza, di elaborare soluzioni nuove, ma non è dotata di pensiero, di morale[142]; quindi non è libera nel suo agire essendo programmata per realizzare degli obiettivi.

[141] La teoria è stata elaborata da G. HALLEVY, *Liability for Crimes Involving Artificial Intelligence System*, 2015; sul punto si vedano anche: M. BASSINI, L. LIGUORI, O. POLLICINO, *Sistemi di Intelligenza artificiale, responsabilità e accountability. Verso nuovi paradigmi?*, in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Milano, 2018, 363 ss.; A. CAPELLINI, *Machina delinquere non potest*, cit., 5 ss.

[142] D. LIMA, *Could AI agents be held criminally liable? Artificial Intelligence and the Challenges for criminal law*, in *South Carolina Law Review*, 2018, 69, 3, 682 ss.

Una parte della dottrina[143] ipotizza il riconoscimento della personalità giuridica della macchina, alla stregua di una "personalità elettronica", che possa assumere rilevanza dal punto di vista giuridico.

Le macchine pensanti - secondo questa teoria - dovrebbero essere identificate attraverso l'inserimento all'interno di un registro e risponderebbero delle obbligazioni e degli eventuali danni grazie ad un fondo patrimoniale istituito *ad hoc*.

Il fondo sarebbe alimentato da coloro che creano, utilizzano o gestiscono la macchina.

Questo meccanismo però, chiama a rispondere di fatto un soggetto diverso dall'autore, in quanto il danno finisce per ricadere sul produttore o sull'utilizzatore richiamando forme di responsabilità vicaria che il diritto penale non può condividere.

L'IA non è un soggetto di diritto, pertanto risulta difficile ipotizzare un tipo di responsabilità autonoma, in quanto verrebbe snaturato il fine ultimo del diritto penale, ossia l'applicazione di una sanzione per fatto proprio colpevole[144].

Anche il parallelismo con la responsabilità della persona giuridica non convince. L'ente risponde per un fatto realizzato nel suo interesse da un soggetto posto in posizione apicale o subordinata, ma la sanzione incide sul

[143] C. PIERGALLINI, *Intelligenza artificiale: da mezzo ad autore del reato?*, cit., 12 ss.

[144] A. CAPELLINI, *Machina delinquere non potest?*, cit., 499 ss.; P. SEVERINO, *Intelligenza artificiale e diritto penale*, Milano, 2020, 535 ss.; R. BORSARI, *Intelligenza artificiale e responsabilità penale: prime considerazioni*, in *Rivista del diritto dei media*, 2019, 3, 262 ss.

profitto che è l'obiettivo essenziale dell'operato aziendale[145]; nel caso dell'IA su cosa inciderebbe la sanzione?

Invero, in dottrina[146] si è sviluppato un orientamento che partendo dalle pregiudiziali ontologiche, poste a fondamento del principio secondo cui *societas delinquere non potest*, mira a dimostrarne l'inconsistenza di fronte alla macchina pensante.

In primo luogo, sostiene che mentre l'ente sarebbe incapace di azione in senso naturalistico, la macchina potrebbe porre in essere autonomamente un fatto di reato (si pensi al movimento di un braccio robotico). In tal senso si abbraccia un'idea di azione sostanzialmente naturalistica.

In secondo luogo, ritiene che da un punto di vista soggettivo la cognizione e volizione si concilino con l'agente artificiale. Come l'agente umano l'IA acquisisce informazioni rielaborando gli *input* che provengono dall'esterno; per quanto riguarda la volizione la macchina è capace di prevedere la realizzazione di un evento ed agire di conseguenza.

Infine, quest'orientamento ipotizza persino una capacità di "pena" dell'IA, che si sostanzia nella privazione della capacità di agire dell'agente artificiale.

---

[145] V. B. BHARGAVA, M. VELASQUEZ, *Is corporate responsibility relevant to Artificial Intelligence Responsibility?*, in *The Georgetown Journal of Law Public Policy*, 2019, 17, 830 ss.; P. SEVERINO, *Intelligenza artificiale e diritto penale*, cit., 535 ss.

[146] Tra gli altri: S. RIONDATO, *Robot, talune indicazioni di diritto penale*, in P. MORO, C. SARRA (a cura di), *Tecnodiritto*; D. LIMA, *Could AI Agents be held criminally liable?*, cit., 688 ss.

L'ipotesi di una diretta responsabilità della macchina sebbene suggestiva presta il fianco a critiche e dubbi che allo stato sembrano essere "ancora" insuperabili.

Innanzitutto, il parallelismo con la responsabilità della persona giuridica sembra essere forzato e privo di fondamento, in quanto la *societas* sebbene esista nella realtà sociale agisce per mezzo dei soggetti che la rappresentano mentre la macchina ha una fisicità ed agisce autonomamente anche se per il tramite di un algoritmo ideato da altri[147].

La fisicità che la contraddistingue può essere ritenuta sufficiente per riconoscerle una capacità di azione, di colpevolezza e di pena?

La capacità di azione - intesa in senso lato - deve essere sorretta dalla volontarietà, o meglio dalla *suitas*; in altre parole, deve essere espressione della capacità di autodeterminazione. Prima che con dolo o colpa, la condotta viene realizzata da un corpo intelligentemente; l'atto è frutto di un comportamento proprio del soggetto.

L'intelligenza artificiale è capace di autoapprendimento, ma si può dire che sia capace di autodeterminarsi?

Alla luce delle attuali evidenze la risposta sembrerebbe essere negativa; pertanto, l'assimilazione dell'IA all'intelligenza umana rimane un'ipotesi

[147] U. PAGALLO, *The Laws of Robots. Crimes, Contracts, Torts*, Dordrecht, 2013, 45 ss.; P.M. FREITAS, F. ANDRADE, P. NOVAIS, *Criminal Liability of Autonomous Agent: From the Unthinkable to the Plausible*, in CASANOVAS-PAGALLO-PALMIRANI-SARTOR (eds), *AI Approaches to the Complexity of Legal Systems*, Berlin-Heidelberg, 2014, 153 ss.

futura che però al momento contrasta con i requisiti minimi del diritto penale[148].

Anche la capacità di colpevolezza risulta essere una pregiudiziale invalicabile.

Ammesso che il comportamento possa essere riferito all'agente artificiale da un punto di vista oggettivo, la rimproverabilità della macchina sarebbe comunque impossibile perché l'IA non è capace di scegliere e non è dotata di libero arbitrio[149].

Infine, si deve sottolineare come anche la funzione della pena non potrebbe realizzarsi nei confronti di un'entità artificiale[150].

Sicuramente la funzione retributiva non può riscontrarsi in una pena robotica, in quanto presuppone una responsabilità colpevole; per la prevenzione generale[151] dovrebbe ipotizzarsi una surreale capacità di deterrenza nei confronti della platea robotica e per la prevenzione speciale[152], la sanzione dovrebbe essere idonea a scongiurare il pericolo di recidiva, dovrebbe essere capace di rieducare la macchina, ma sarebbe possibile? In che modo?

---

[148] S. GLESS, E. SILVERMAN, T. WEIGEND, *If Robots Cause Harm, who is to blame? Self-driving cars and criminal liability*, in *New Criminal Law Review*, 2018, 677 ss.

[149] M. HILDEBRANDT, *Autonomic and autonomous thinking. Preconditions for criminal accountability*, in *Hildebrandt, Rouvroy, Law, Houman Agency and Autonomic Computing*, Abingdon, 2011, 141 ss.

[150] P. M. ASARO, *A body to kick, but Still No Soul to Damn: Legal Perspective on Robotics*, in LIN, ABNEY, BEKEY, *Robot Ethics*, Cambridge, 2012, 169 ss.

[151] P. M. ASARO, *Determinism, machine agency, and responsibility*, in *Politica e società*, 2014, 282 ss.

[152] Sul punto: HALLEVY, *Liability for Crimes Involving Artificial Intelligence Systems*, cit., 210 ss.

Ecco anche nei casi estremi di "morte elettronica" dell'agente artificiale[153], cioè nel caso della sua disattivazione, sarebbe impossibile rieducare l'IA, perché la macchina è ontologicamente incapace di pensare e di comprendere i propri errori e di imparare dagli stessi.

Alla luce di queste prime considerazioni, si può dire che allo stato a risponderne è sempre l'agente umano, in qualità di programmatore o di utilizzatore, però sorge spontaneo un interrogativo: a che titolo è chiamato a risponderne?

3.1.2 La responsabilità colposa dell'operatore per comportamenti autonomi della macchina: l'*explainability*.

L'assenza di soggettività giuridica e di una "morale" riferibile all'agente artificiale - come si è visto - determina l'impossibilità di muovere un rimprovero nei suoi confronti.

Orbene, la necessità di riconoscere una responsabilità in capo all'agente umano deve però, essere delineata in conformità con i principi cardine del diritto penale ed in particolare con il principio di colpevolezza.

I soggetti che vengono in rilievo sono: il programmatore, l'utilizzatore ed il titolare della macchina[154].

---

[153] C. PIERGALLINI, *Intelligenza Artificiale: da mezzo ad autore del reato?*, cit., 17 ss.

[154] M. B. MAGRO, *Decisione umana e decisione robotica. Un'ipotesi di responsabilità da procreazione robotica*, in *La legislazione penale*, 2020.

Per quanto riguarda il programmatore per poter muovere un rimprovero per colpa bisognerebbe estendere al massimo i principi di prevedibilità ed evitabilità dell'evento, per poter ipotizzare una responsabilità da prodotto difettoso, cadendo quasi sicuramente in una forma di responsabilità oggettiva[155].

Il rischio di muovere un rimprovero pur in assenza di colpa in capo al programmatore sussiste perché, come si è visto, le macchine intelligenti arrivano a risultati non sempre prevedibili *ex ante*; alla luce di queste considerazioni sembra anacronistico riconoscere una responsabilità in assenza di prevedibilità e quindi evitabilità in capo all'agente.

Per motivi diversi appare complesso lo schema di imputazione per il proprietario e l'utilizzatore[156].

Negli ordinamenti di *common law* si fa riferimento a forme di *strict liability*, fondate sul criterio del *respondeat superior*[157], ma tale tipo di modello non può essere adottato da sistemi di *civil law*, per contrasto con l'ordinamento costituzionale.

[155]F. LAGIOIA, G. SARTOR, *AI system under criminal law: a Legal Analysis and a Regulatory Perspective*, in *Philosophy and Technology*, 2020.

[156] P. M. ASARO, *A body to kick, but Still No Soul to Damn: Legal Perspective on Robotics*, cit., 179.

[157] J. HORDER, *Ashworth's Principles of criminal law*, 9th ed., 2019, 181; A. CADOPPI, C. M. PRICOLO, *Strict Liability nel diritto anglo-americano (voce)*, in *Dig. Pen*., vol. XIV, Torino, 1999, 20 ss.

Si richiede la sussistenza almeno di una responsabilità a titolo di colpa[158] che per come operano gli agenti artificiali è di difficile individuazione.

Per questo motivo è necessario un cambio di paradigma per poter colmare il c.d. *responsibility gap*[159].

Ipotizzare una responsabilità dolosa è semplice nel caso in cui l'agente artificiale venga progettato per commettere reati; trattandosi di un fatto che appartiene al proprio autore ed essendo l'IA un mero strumento per perpetrare il reato si pone fuori dalla c. d. autoria mediata.

Quando l'agente umano - a seconda del tipo di autonomia di cui è dotato l'algoritmo - non ha signoria sulla macchina si parla di responsabilità colposa in quanto lo schema del dolo, che necessita di rappresentazione e volizione, non sembra in alcun modo ipotizzabile.

Nel caso in cui l'agente artificiale non abbia capacità di autoapprendimento e non sia autonomo lo schema della colpa risulta facilmente rinvenibile; si pensi all'errore di programmazione o funzionamento che potrà essere imputato a coloro che hanno programmato, sviluppato, prodotto o collaudato la macchina.

---

[158] T. C. KING, N. AGGARWAL, M. TADDEO, L. FLORIDI, *Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions*, in *Science and Engineering Ethics*, 2020, 26, 94 ss.

[159] J. DANAHER, *Robots, Law and the Retribution Gap*, in *Ethics and Information Technology*, 2016, 18,4, 299 ss.; A. MATTHIAS, *The responsibility gap: Ascribing responsibility for the actions of learning automata*, in *Ethics and Information Technology*, 2004, 6, 175 ss.

Il discorso cambia nel caso in cui l'IA sia completamente autonoma rispetto all'agente umano, in quanto risulta difficile ricostruire i concetti di prevedibilità ed evitabilità dell'evento quando ad agire è una macchina.

In questo caso, l'interrogativo principale è: *machina delinquere potest*?

Orbene, la prima difficoltà riscontrata, risiede nell'individuazione della regola cautelare violata[160] - date le peculiarità del soggetto agente - ma si può dire che complessa sia anche la ricostruzione della correlazione normativa che deve legare la violazione cautelare e l'evento.

Un altro aspetto importante riguarda la pluralità di soggetti che si interfacciano con la macchina che rende necessario individuare il soggetto cui imputare il fatto di reato proprio perché ciascuno svolge un pezzo del processo funzionale all'operatività della macchina[161].

Risulta difficile enucleare la regola cautelare cui devono uniformarsi gli agenti umani poiché in caso di reato "posto in essere" dall'IA oltre al momento lesivo di diritti altrui esiste una fase esecutiva in cui l'algoritmo raccoglie i dati, crea un modello ed esegue l'azione.

In questo caso ragionare in termini di prevedibilità ed evitabilità dell'evento per la persona fisica appare complesso.

---

[160] C. PIERGALLINI, *Danno da prodotto e responsabilità penale, Profili dogmatici e politico-criminal*i, Milano, 2004, 12 ss.

[161] V. ATTILI, *L'agente-modello "nell'era della complessità": tramonto, eclissi o trasfigurazione?*, in *Riv. It. Dir e proc. pen*., 2006, 4, 1240 ss.

Una parte della dottrina[162] sottolinea come in questo caso assuma rilevanza il comportamento che si auspica sia tenuto dall'agente, al di là della diligenza necessaria ad evitare l'evento; in altri termini, viene valorizzata la decisione presa dall'operatore per poi costruire un eventuale addebito di responsabilità. In questo scenario nasce e si sviluppa il concetto di *responsability gap*, ma come è possibile evitare che il c.d. *gap* si verifichi?

Si ritiene che un primo intervento debba essere realizzato a livello normativo, a tal proposito una possibile soluzione potrebbe essere l'*IA Act*, che si propone di disciplinare principi e regole che governano i processi di creazione e funzionamento delle tecnologie di IA; in una seconda fase, si potrebbe prospettare un intervento settoriale, prendendo in considerazione classi di comportamenti che corrispondono a singole categorie di reati.[163]

3.1.3 Soluzioni prospettabili per il *responsability gap*.

Di fronte all'inarrestabile avanzamento della tecnologia, in dottrina si sono sviluppate diverse teorie per cercare di superare il c.d. *responsability gap*.

In primo luogo, si è ipotizzata una limitazione della responsabilità degli operatori[164]; alla base di questa teoria si pone l'autonomia della decisione

[162] C. PIERGALLINI, voce *Colpa (diritto penale)*, in *Enc. Dir. Annali*, X, 2017, 224 ss.

[163] Sul punto si segnala il contributo fornito dal Working Group su IA e diritto penale elaborato per *l'European Committee on Crime Problems* del Consiglio d'Europa: *Feasibility Study on a future Council of Europe Instrument on Artificial Intelligence and Criminal Law*, CDPC, 4 settembre 2020.

[164] S. GLESS, E. SILVERMAN, T. WEIGEND, *If robots cause harm, who it to blame? Self-driving Cars and Criminal Liability*, in *New Criminal Law Review*, 2016, 430 ss.

della macchina; quindi, si considera l'azione dell'IA autonoma rispetto all'agente umano, al pari di una causa sopravvenuta capace da sola di determinare l'evento operando un'interruzione del nesso causale tra la condotta dell'agente umano e l'evento.

Tale prospettiva presenta molteplici criticità[165]; infatti, non considera che una responsabilità colposa in capo all'operatore potrebbe in ogni caso sussistere e non si sofferma sul rischio di comportamenti emergenti volutamente prospettati dall'agente umano al momento della progettazione.

Tale ipotesi deresponsabilizza sia l'agente artificiale che quello umano, pertanto, non sembra giuridicamente ed eticamente corretta, in quanto lascerebbe le vittime dell'illecito prive di adeguata tutela[166].

La seconda soluzione prospettata dalla dottrina si basa sull'attenuazione del dovere di diligenza che si impone all'operatore nel momento in cui quest'ultimo abbia rispettato gli obblighi stabiliti dall'ordinamento[167].

Il presupposto per applicare tale teoria si fonda sulla capillare diffusione della tecnologia e sull'accettazione da parte della società della permanenza di un rischio residuo in seguito al funzionamento dei sistemi basati sull'intelligenza

---

[165] C. PIERGALLINI, *Intelligenza artificiale*, cit., 1745 ss.

[166] B. PANATTONI, *Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'autonomia artificiale*, in *Dir. dell'informazione e dell'informatica*, II, 317 ss.

[167] S. GLESS, E. SILVERMAN, T. WEIGEND, *If robots cause harm, who it to blame?*, cit., 430 ss.

artificiale; in altre parole, la società si fa carico dei rischi derivanti dal funzionamento della macchina[168].

Orbene, sembrerebbe che anche tale teoria tenda a trattare in modo eccessivamente semplicistico il problema e non tenga conto del fatto che spesso gli interessi lesi dall'operatività della macchina sono interessi fondamentali dell'individuo.

A questo punto, gli interpreti si chiedono quale sia il ruolo del diritto penale nella società del rischio; il dibattito ha fatto emergere varie teorie: la prima prevede il ricorso al solo illecito amministrativo[169], a questa si contrappone l'ipotesi che considera irrinunciabile il ricorso al diritto penale[170] ed infine una terza teoria che sostiene la possibilità di prevedere un modello misto tra illecito penale ed amministrativo[171].

La questione rimane ancora aperta, ma nel prosieguo del lavoro si cercherà di capire quali possono essere gli utilizzi delle nuove tecnologie in ambito aziendale: in primo luogo, da un punto di vista organizzativo ed in secondo luogo, in un'ottica preventiva.

---

[168] A. CAPELLINI, *Profili penalistici delle self-driving cars*, in *Dir. pen. cont*., 2019, 326 ss.

[169] Si veda F. STELLA, *Giustizia e modernità. La protezione dell'innocente e la tutela delle vittime*, Milano, 2003, 593 ss.

[170] G. MARINUCCI, *Innovazioni tecnologiche e scoperte scientifiche costi e tempi di adeguamento delle regole di diligenza*, in *Riv. It. Dir. e proc. pen*., 2005, 29 ss.

[171] C. PONGILUPPI, *Principio di precauzione e diritto penale: nihil novi sub sole?*, in *Dir. pen. cont*., 2009, 252 ss.

CAPITOLO III

Le nuove tecnologie al servizio delle imprese. Quali prospettive per la *criminal compliance*?

SOMMARIO: 1. Intelligenza artificiale e *criminal compliance* a livello aziendale. - 1.1 Dalla FinTech alla CorpTech. - 1.2 La digitalizzazione dei processi aziendali. - 1.3 La mappatura delle aree a rischio reato tramite l'IA. La digitalizzazione del modello organizzativo. - 2. *Blockchain* e *criminal compliance*. - 2. 1 L'analisi dei flussi informativi. - 2.2 L'impiego dei DLT nei processi finanziari aziendali. - 3. L'utilizzo di sistemi automatizzati nella fase di *risk assestment* e di *risk management*. - 4. Gli obblighi imposti dalla normativa in tema di tutela della *privacy*. - 5. Come conciliare la *digital criminal compliance* con la tutela dei diritti dei soggetti coinvolti dall'analisi dei dati? - 6. La possibile automatizzazione delle investigazioni interne: problemi e prospettive. - 7. Un approccio casistico.

1. Intelligenza artificiale e *criminal compliance* a livello aziendale.

L'intelligenza artificiale – come si è visto – è un termine che include una pluralità di tecniche e di *software* che hanno caratteristiche e proprietà diverse, ma rappresentano una grande opportunità per lo sviluppo di molti settori nell'ambito dell'industria 4.0.

Il dibattito relativo all'utilizzo dell'IA in ambito penale si sta alimentando anche nel nostro ordinamento, sulla base dell'evoluzione che ha avuto a partire dai sistemi di *common law* americani; in questa sede, si analizzerà lo stato dell'arte e gli sviluppi che si intravedono all'orizzonte rispetto all'utilizzo di strumenti algoritmici per l'attività di *compliance* a livello aziendale.

La valutazione e gestione del rischio reato richiede cospicui investimenti da parte delle imprese, ma soprattutto necessita di un sistema capace di analizzare grandi masse di informazioni; l'utilizzo dei *software* basati sull'intelligenza artificiale agevolerebbe la mappatura delle aree a rischio reato grazie all'analisi massiva dei dati; ma potrebbe avere un ruolo determinante anche nella rilevazione di condotte illecite *ex ante*, in quanto un *compliance program* automatizzato rende – in astratto – più difficile l'elusione delle regole da parte dei soggetti che a vario titolo operano all'interno della compagine aziendale.

Questi ad una prima analisi potrebbero essere i vantaggi, ma sicuramente dietro l'utilizzo dei sistemi artificiali si celano plurimi rischi.

L'ente potrebbe essere accusato di una mancata attuazione del modello nel momento in cui sia rimasto inerte di fronte ad un pericolo segnalato dalla macchina e da un punto di vista diametralmente opposto, potrebbe essere ritenuto responsabile nel momento in cui la macchina non abbia rilevato un rischio nell'ambito di una determinata operazione che porti alla commissione di un illecito ai sensi del catalogo 231; in questo caso *quid iuris*?

Ecco, si deve rilevare che nei casi richiamati la persona giuridica potrebbe essere ritenuta responsabile per un'attività realizzata da un *software* costruito da altri, violando i criteri stabiliti dall'ordinamento per il riconoscimento della colpa di organizzazione[172]; nei prossimi paragrafi si cercherà di capire come

[172] Sul punto si veda cap. I del presente lavoro.

la tecnologia possa mettersi al servizio dell'impresa senza eludere i meccanismi di imputazione della responsabilità previsti.

1.1 Dalla FinTech alla CorpTech.

Il primo settore che ha visto un vasto impiego di strumenti di intelligenza artificiale è quello finanziario. Il nuovo mercato finanziario basato su prodotti e servizi digitalizzati viene conosciuto come FinTech[173].

Il minimo comune denominatore di tale processo riguarda l'applicazione degli strumenti tecnologici alla realtà della finanza; nello specifico ci si riferisce a servizi di *analytics*, *chatbot*, *machine learning*, *cognitive computing*[174], che consentono di realizzare operazioni sul mercato in maniera sempre più rapida ed efficiente.

Plurimi sono gli impieghi delle tecnologie nel settore finanziario: si pensi ai servizi di credito, di pagamento, di consulenza etc.

L'utilizzo dell'IA rappresenta una risorsa per le società che operano nell'ambito della FinTech soprattutto per la gestione del rischio, c.d. *risk managment*; in quanto, gli algoritmi consentono di effettuare delle previsioni

[173] G. ALPA, *FinTech: un laboratorio per i giuristi*, in *Contr. Impr*., 2019, 378; S. ALVARO – L. MARZIALETTI – D. TUZZOLINO, *Evoluzioni normative fra policy e diritto*, in *La portabilità dei dati in ambito finanziario*, a cura di A. GENOVESE e V. FALCE, in *Quaderni FinTech*, www.consob.it.

[174] A. NATALE, *Intelligenza artificiale e finTech: profili di responsabilità*, Milano, 2022, 43 ss.

molto specifiche e settoriali partendo dai dati esistenti, riducendo la possibilità di esposizione all'aleatorietà del mercato.

La tecnologia consente la gestione del portafoglio del cliente in forma automatizzata, ma anche di stipulare ed eseguire contratti in forma di *smart contract*, favorendo la profilazione dei clienti ed una più efficace valutazione dei rischi; ad esempio, il rischio riciclaggio.

Nel campo del credito le banche e gli intermediari finanziari hanno il compito di valutare l'affidabilità dei soggetti che vi si rivolgono per un finanziamento; l'utilizzo di algoritmi consente di valutare i potenziali clienti in maniera più pervasiva e sostanziale[175] potendo basare l'analisi su grandi quantità di informazioni processate in forma automatizzata.

L'intelligenza artificiale rappresenta uno strumento valido anche per prevenire eventuali frodi, grazie al suo utilizzo nell'ambito delle transazioni e dei pagamenti, in quanto consente una rapida verifica e segnalazione delle prestazioni anomale.

Per quanto riguarda l'automatizzazione dei pagamenti parte della dottrina[176] osserva che da un punto di vista giuridico si assiste ad una trasformazione dell'atto di pagamento che da adempimento dell'obbligazione sembra divenire un'operazione quasi inconsapevole, realizzata esclusivamente sulla

[175] Sul punto si veda: R. MANCINI, *L'intelligenza artificiale nel credit scoring finanziario e assicurativo*, in *XXVI lezioni di diritto dell'intelligenza artificiale*, a cura di U. RUFFOLO, 2021, 706 ss.

[176] Si esprime in tal senso N. ABRIANI – G. SCHNEIDER, *Diritto delle imprese e intelligenza artificiale*, Bologna, 2021, 123 ss.

base di un percorso identificato dalla macchina. Sicuramente, di fronte ad un cambiamento di questa portata si rende necessaria una maggiore responsabilizzazione del cliente per un'esigenza di tutela dai rischi di *bias* comportamentali.

Invero, un ambito in cui gli algoritmi vengono sempre di più utilizzati è quello della consulenza, si parla della c.d. *robot advisory*[177]; quest'ultima si propone di supportare le decisioni adottate da soggetti "umani" con l'analisi dei dati.

L'IA ha la possibilità di effettuare controlli massivi dei dati e di farlo in modo obiettivo senza subire alcun tipo di influenza esterna ed emozionale.

Un'altra innovazione che si è avuta in ambito finanziario è data dall'introduzione di valute virtuali gestite mediante piattaforme automatizzate e negoziate su mercati non regolamentati; l'esempio classico sono i *bitcoin* e i *token*[178].

Insomma, ad una prima analisi si può osservare che le tecnologie applicate al settore finanziario hanno avuto uno sviluppo molto pervasivo trasformando il mercato e favorendo l'ingresso di nuovi soggetti ed operatori.

Si deve specificare che se da un lato le istituzioni preposte hanno sviluppato delle soluzioni per risolvere specifici problemi o lacune tipiche del settore finanziario dall'altro le grandi imprese digitali hanno utilizzato dei sistemi già esistenti adattandoli alle nuove esigenze del mercato.

---

[177] A. NATALE, *Intelligenza artificiale e fintech: profili di responsabilità*, cit., 45.

[178] S. ALVARO – L. MARZIALETTI – D. TUZZOLINO, *Evoluzioni normative fra policy e diritto*, in *La portabilità dei dati in ambito finanziario*, a cura di A. GENOVESE, cit.

A tal proposito, bisogna distinguere i servizi FinTech da quelli TechFin[179]; i primi, sono studiati da esperti del settore finanziario e creati originariamente per essere utilizzati in questo; i secondi, attengono al digitale in generale e vengono adattati al campo della finanza.

Il valore aggiunto dei servizi TechFin risiede nella riduzione delle asimmetrie informative. Le grandi società digitali[180] utilizzano i dati di indicizzazione che carpiscono dai consumatori per profilare gli interessi commerciali e creditizi degli stessi; in altre parole, posseggono - e di conseguenza sfruttano - un patrimonio di dati e informazioni cui le *startup* e le società finanziarie non possono accedere se non a caro prezzo.

Le società che adoperano servizi TechFin hanno il privilegio di rivolgersi ad un numero più ampio di utilizzatori, ma ad un minor prezzo, ovviamente la profilazione dei clienti poiché adopera tecniche di indicizzazione non è esente da rischi, in quanto potrebbero essere effettuate delle predizioni erronee e discriminatorie basate su informazioni che attengono al genere, all'età oppure all'etnia dei consumatori[181].

L'utilizzo delle tecnologie nel settore finanziario ha determinato parallelamente lo sviluppo di forme di utilizzo di strumenti tecnologici a fini regolatori, di *compliance*, di vigilanza dando vita alla c.d. ReghTech[182].

---

[179] G. ALPA, *Fintech: un laboratorio per giuristi*, cit., 378.

[180] Si fa riferimento a Google, Amazon ed ai *social network* più diffusi.

[181] N. ABRIANI - G. SCHNEIDER, *Diritto delle imprese e intelligenza artificiale,* cit., 125 ss.

[182] Per un'analisi del passaggio dalla TechFin alla FinTech si veda: G. ALPA, *Fintech: un laboratorio per giuristi*, cit., 379.

Il fenomeno nasce in risposta alle nuove esigenze di regolazione del settore finanziario e determina l'abbattimento dei costi connessi all'attività di supervisione e di controllo dei fornitori di strumenti finanziari consentendo allo stesso tempo un'attività di controllo indiretto del mercato.

Le caratteristiche positive della ReghTech consistono nell'analisi massiva dei dati, nella capacità di generare *report* in tempo reale, ma la vera svolta per i sistemi di memorizzazione e di controllo riguarda il trasferimento su *cloud* del materiale informativo che viene posto alla base delle attività regolatorie.

Nel tempo si è avuta un'ampia diffusione di soluzioni tecnologiche sia per la comunicazione dei flussi informativi tra i vari dipartimenti oppure tra le imprese appartenenti al gruppo (ComplianceTech), sia per la realizzazione di procedure interne (OperationsTech).

Spesso gli strumenti tecnologici adoperati per garantire la *compliance* e la correttezza delle operazioni sono incorporati nei *software* FinTech per consentire una proficua operatività dall'interno.

Parte della dottrina sostiene che un limite all'illegittimità del comportamento dipende dalle impostazioni del *software* ReghTech[183], ma soprattutto dal fatto che la sanzione conseguente alla violazione è maggiore del beneficio apportato alla società dall'operazione contrastante con le regole di *compliance.*

[183] N. ABRIANI - G. SCHNEIDER, *Diritto delle imprese e intelligenza artificiale,* cit., 130 ss.

L'utilizzo di nuove tecnologie nell'ambito della compliance ha determinato la necessità di sviluppare *software* idonei alla supervisione degli strumenti di *ComplianceTech* e di *OperationsTech*.

L'attività di regolazione non sembra essere più improntata esclusivamente al controllo di decisioni umane, ma è rivolta alla supervisione della tecnologia tramite la tecnologia stessa.

L'esigenza di sviluppare *software* ReghTech[184] ha determinato l'adozione di soluzioni diverse da parte delle imprese e delle autorità regolatorie; infatti, a soluzioni create da soggetti terzi si sono affiancati sistemi realizzati dalle stesse aziende.

In quest'ultimo caso, si pone un problema di coincidenza tra regolatore e regolato che determina una potenziale situazione di conflitto di interessi; inoltre, l'autoregolazione comporta delle difficoltà da un punto di vista tecnico per la mancanza di soggetti dotati delle necessarie competenze in vista della progettazione ed attuazione dello strumento di regolazione.

Il problema del conflitto di interessi si pone principalmente per le autorità pubbliche che si affidano a soggetti privati che spesso costruiscono sistemi di regolazione tesi a realizzare più gli interessi delle imprese regolate che delle società regolatrici; da questo punto di vista, la possibile soluzione potrebbe essere disciplinare in maniera pedissequa *ex ante* i caratteri del contratto di

[184] L. ENRIQUES, *Financial Supervisors and RegTech: Four Roles and Four Challenges*, in *"RTDF"*, 2017, 53 ss.; N. ABRIANI - G. SCHNEIDER, *Diritto delle imprese e intelligenza artificiale* 134 ss.

committenza degli strumenti regolatori pur sapendo che in questo settore tali accorgimenti non rappresentano la "svolta definitiva".

Sebbene il rischio connesso al conflitto di interessi sia pregnante si deve sottolineare che la ReghTech determina anche una serie di effetti positivi: si pensi, al costante dialogo tra regolatori e regolati ed alle opportunità di confronto che consentono non solo un proficuo impiego delle tecnologie, ma anche il corretto funzionamento dei mercati.

Quindi possiamo dire che lo sviluppo della FinTech ha determinato la nascita di soluzioni regolatorie che utilizzassero prevalentemente l'intelligenza artificiale in modo da esercitare un adeguato controllo sulle imprese operanti sul mercato; la tecnologia, però, ha contribuito a ripensare le modalità di gestione ed amministrazione delle società, tale fenomeno secondo la dottrina prevalente prende il nome di CorpTech[185].

Quest'ultima viene definita come l'insieme degli strumenti tecnologici di cui il CdA può dotare l'impresa a fini amministrativi.

Tra le varie tecnologie è stato osservato che l'intelligenza artificiale è quella che più si presta ad essere adoperata nel contesto aziendale come ausilio alle scelte gestionali. L'IA può essere adoperata nella fase successiva rispetto

[185] Tra gli altri: N. ABRIANI - G. SCHNEIDER, *Diritto delle imprese e intelligenza artificiale* 140 ss.; ID., *Successo sotenibile e regole statutarie: il ruolo del board nel Codice di Corporate Governance*, in *"Rivista di Corporate Governance",* I, 2021, 17-18.

all'adozione di scelte strategiche e non per sostituire i decisori nella determinazione delle scelte di fondo[186].

L'IA viene impiegata nell'ambito della *corporate governance*; quest'ultima comprende l'insieme di regole utili per il funzionamento del Consiglio di Amministrazione. Il pregio della tecnologia è dato dalla capacità di reagire a *input* predefiniti, ma allo stesso tempo di identificarne di nuovi che necessitano di adeguata risposta.

Gli strumenti di intelligenza artificiale - come si è visto nei capitoli precedenti - spesso, sono capaci di autoapprendere e di generare risposte non prevedibili *ex ante*; inoltre, l'IA è alimentata dai dati, pertanto, oltre a dipendere dalla qualità degli stessi è suscettibile di manipolazione da parte di terzi, estranei alla *governance* della società.

L'utilizzo della tecnologia per la gestione della società determina - secondo parte della dottrina[187] - un necessario incremento di professionalità e competenze tra i soggetti appartenenti all'organo amministrativo, la formazione di un comitato *tech* oppure l'accrescimento delle funzioni del comitato di controllo rischi.

I temi accennati verranno approfonditi nei prossimi paragrafi con l'obiettivo di delineare le possibili evoluzioni della tecnologia nel contesto aziendale, ma

[186] In questo senso: U. TOMBRARI, *Intelligenza artificiale e corporate governance nella società quotata*, in *Dir. soc*., 2021, 1431.
[187] A. NATALE, *Intelligenza artificiale e fintech: profili di responsabilità*, cit., 49.

soprattutto nell'ambito della prevenzione del rischio reato ai sensi del d.lgs. 231 del 2001.

1.2 La digitalizzazione dei processi aziendali.

Le nuove tecnologie hanno avuto un rapido sviluppo nel settore finanziario e - come si è visto - ciò ha portato al passaggio dalla FinTech, alla RegTech e poi alla CorpTech, determinando una netta apertura degli orizzonti e facendo emergere a pieno le potenzialità degli algoritmi per le imprese.

Prima di passare all'approfondimento del tema ci si è chiesti cosa si intende per digitalizzazione dei processi aziendali?

In primo luogo, si deve chiarire che il termine digitalizzazione può assumere tre possibili declinazioni: *digitization*, *digitalization e digital transormation*[188].

La *digitization*[189] fa riferimento al passaggio della gestione delle informazioni in forma digitale, in modo da lavorarle in forma telematica; in altre parole, l'opinione prevalente ritiene che il termine *digitization* indichi la conversione in digitale della documentazione interna ed esterna all'azienda[190].

---

[188] M. RUBINO - F. VITOLLA - N. RAIMO, *Il processo di digitalizzazione aziendale e la digital transformation*, 2020, 56.

[189] D. DOUGHERTY – D. DUNNE, *Digital science and Knowledge boundaries in complex innovation. Organization Science*, Vol. 23, n. 5, 1467-1484; C. LOEBBECKE – A. PICOT, *Reflections on societal and business model transformation arising from digitization and big data analytics: A research agenda*, in *Journal of Strategic information Systems*, vol. 24, n. 3, 149-167.

[190] F. LI – A. NUCCIARELLI – S. RODEN – G. GRAHAM, *How smart cities transform operations models: A new research agenda for operations management in the digital economy*, in *Production Planning e Control*, vol. 27, n. 6, 514-528.

Invece, la *digitalization*[191] indica il cambiamento dei processi aziendali tramite le nuove tecnologie.

Quindi si può dire che la digitalizzazione assume un'accezione più ampia in quanto, riguarda l'utilizzo delle nuove tecnologie al fine di ottimizzare i processi esistenti.

Infine, la *digital transformation*[192] rappresenta la forma più pervasiva delle modifiche apportate dalla tecnologia. La DT modifica il modo di gestire e di pensare i processi aziendali determinando un cambiamento nel *business* e nella creazione di valore.

In dottrina non si è sviluppato un orientamento unanime riguardo il significato da attribuire al termine *digital trasformation,* ma sono stati identificati dei tratti comuni[193]: la DT promuove una modifica delle operazioni aziendali coinvolgendo le competenze esistenti, ma creandone anche di nuove; inoltre, interessa l'intero assetto organizzativo e gestionale ed è volta alla

[191] M. PAGANI - C. PARDO, *The impact of digital technology on relationships in a business network*, in *Industrial Marketing management*, vol. 67, 185-192; P. C. VERHOEF – T. BRORKHUIZEN – Y. BART – A. BHATTACHARYA – J. Q. DONG – N. FABIAN – M. HAENLEIN, *Digital transformation: A multidisciplinary reflection and research agenda*, in *Journal of Business Research*, 2019, 1-13.

[192] R. AMIT – C. ZOTT, *Value creation in e-business. Strategic management journal*, vol. 22, n. 6-7, 493-520; L. LI – F. SU – W. ZHANG – J. Y. MAO, *Digital transformation by SME enterpreneures: A* capability perspective, in Information Systems Journal, vol. 28, n. 6, 2018, 1129-1157.

[193] G. WESTERMAN - C. CALMÈJANE – D. BONNET – P. FERRARIS – A. MCAFEE, *Digital transformation: a road-map for a billion-dollar organizations, MIT Center for Digital Business and Capgemini Consulting*, Cambdrige, 2011; L. S. DALENOGARE - G. B. BENITEZ - N. F. AYALA – A. G. FRANK, *The expected contribution of Industry 4.0 technologies for industrial performance*, in *International Journal of Production Economics*, vol. 24, 2018, 383-394.

realizzazione di nuovo valore migliorando, principalmente, i rapporti con gli *stakeholder*.

Orbene, alla luce della rivoluzione digitale che sta investendo tutti i settori, coinvolgendo tutte le sfaccettature della vita sociale ed economica, le imprese ripensano le proprie attività nel contesto digitale creando nuove forme di valore[194].

Le aziende adottano varie forme di cambiamento della strategia di *business* e conseguentemente del rapporto con il cliente[195].

Il modello di *business* indica l'insieme degli elementi attraverso cui un'azienda crea e distribuisce valore in modo da ottenere un vantaggio competitivo.

L'economia digitale si basa sui dati, pertanto, le imprese hanno la necessità non solo di reperire dati, ma anche di elaborarli; rispetto a questo processo fondamentale è la *Big data analytics*, in quanto consente di analizzare rapidamente le informazioni e di prevedere i possibili comportamenti dei clienti, in modo da generare valore in termini di competitività sul mercato.

La tecnologia fornisce un valore aggiunto anche in termini di archiviazione riducendone i costi e semplificando l'attività grazie al *cloud computing*.

[194] C. ZOTT – R. AMIT, *Business Model Innovation – How to create Value in a Digita*l *World*, in *GfK Marketing Intelligence Review*, vol. 9, n. 1, 2017, 18-23.

[195] M. RUBINO – F. VITOLLA – A. GARZONI, *Cultura nazionale e livello di digitalizzazione delle imprese europee: evidenze empiriche in Identità, innovazione e impatto dell'aziendalismo italiano*, a cura di F. CULASSO, M. PIZZO, Università di Torino.

L'impatto sui processi aziendali dei sistemi digitali è sicuramente notevole e sebbene rappresenti un'opportunità cela dei rischi che l'impresa deve mettere in conto ed affrontare.

Una parte della dottrina[196] osserva che l'azienda deve porsi degli obiettivi di breve periodo in quanto i vantaggi competitivi che possono essere raggiunti mediante la tecnologia sono estremamente volatili. Le aziende del settore ragionano ed agiscono per imitazione pertanto è necessario implementare delle tecniche di rapida valorizzazione ed altrettanto celere ricostruzione del vantaggio quando quest'ultimo sarà andato perso.

Quindi, si può dire che le aziende per rispondere alle esigenze di innovazione e di progresso che il mercato richiede, devono rivedere e ripensare l'intera strategia aziendale[197].

---

[196] D. IACOVENE, *La trasformazione dei modelli di business nell'era digitale*, Bologna, 2018.

[197] Analizza le modalità per ripensare la strategia aziendale M. RUBINO, *Il processo di digitalizzazione aziendale e la digital transformation*, in *Smart Technologies, Digitalizzazione e Capitale Intellettuale* (a cura di) R. LOMBARDI - M.S. CHIUCCHI - D. MANCINI, 2020, secondo l'Autore: la competitività del mercato rende necessaria una approfondita valutazione degli elementi chiave della strategia: ad esempio, la clientela, la gestione, l'analisi dei dati, la concorrenza ed i valori aziendali.
Deve essere rimodulato l'approccio al cliente in quanto, non può più essere strutturato in maniera uguale per tutti ma è necessario che l'offerta sia personalizzata; per quanto riguarda la concorrenza, ha osservato l'Autore che non può essere vista in costante contrapposizione con la cooperazione aziendale in quanto, le nuove tecnologie hanno cambiato il modo di pensare il *business* imprenditoriale pertanto, potrebbe succedere che un concorrente abbia dei procedimenti che si intersecano con quelli dell'azienda cui si appartiene rendendo sfumati i confini ed incentivando forme di interrelazione; un altro pilastro su cui si forma la strategia digitale è l'analisi dei dati. Le aziende gestendo i dati in forma digitale hanno la possibilità di sfruttarne al meglio il valore strategico e di conseguire un vantaggio competitivo sul mercato. L'Autore ritiene che la proposta di valore debba essere sempre aggiornata e grazie alle tecnologie digitali sarà possibile realizzare un costante aggiornamento che tenga conto ed anticipi le mosse dei concorrenti e si adatti velocemente alle contingenze.

1.3 La mappatura delle aree a rischio reato tramite l'IA. La digitalizzazione del modello organizzativo.

Le nuove tecnologie hanno determinato un cambiamento nel modo di pensare i processi aziendali, ma rappresentano una risorsa anche per la prevenzione del rischio reato.

Ai sensi del d.lgs. 231 del 2001, la persona giuridica andrà esente da responsabilità qualora dimostri di aver adottato ed efficacemente attuato un modello di organizzazione e gestione che risulti essere idoneo a prevenire reati della specie di quello verificatosi.

L'utilizzo della tecnologia potrebbe contribuire a realizzare l'efficienza in termini non solo quantitativi, ma soprattutto qualitativi.

Nella "costruzione" del modello entrano in campo – oltre al giurista – gli esperti di materia[198] e nel caso di applicazione dell'IA, il coinvolgimento dei vari "attori", potrebbe contribuire a realizzare il "modello matematico 231"[199].

[198] R. TREZZA, *I Valori giuridici possono mai trasformarsi in variabili algoritmiche? Brevi osservazioni su giurimetria, algo-crazia e algoretica*, in www.intelligenzaartificiale.unisal.it; G. DALIA, L'esperienza italiana nella lotta alla corruzione: prevenzione, sanzione penale, contrasto processuale e performance, in *Iura and legal systems*, n. 4/2019, 27-31.

[199] Parla di "modello matematico": R. TREZZA, *L'intelligenza artificiale come ausilio alla standardizzazione del modello 231: vantaggi "possibili" e rischi "celati"*, in *Giurisprudenza Penale web*, 2021, 1-bis.

La realizzazione del modello prevede una prima fase di mappatura delle aree a rischio reato[200]; a tal proposito, ci si chiede se questa fase possa essere completamente automatizzata.

Sicuramente, l'agente artificiale rappresenta un ausilio importante, ma necessita sempre di un controllo esterno; in altre parole, il modello non può essere completamente automatizzato perché, in taluni casi, sono necessarie delle valutazioni che in concreto la macchina non ha la possibilità di fare.

Una parte della dottrina[201] ipotizza la standardizzazione dei processi algoritmici destinati alla mappatura delle aree a rischio reato.

Tale ipotesi risulta percorribile qualora le aziende operassero nello stesso settore e fosse effettuato uno studio preliminare di rischiosità.

La standardizzazione delle variabili di rischio potrebbe comportare l'adozione di protocolli unitari[202] diretti alla programmazione, alla formazione ed alla attuazione delle decisioni dell'ente.

Si è però osservato che l'unitarietà delle regole può essere di ausilio nella fase preventiva e di accertamento - in quanto, l'algoritmo consentirebbe di rilevare anomalie di comportamento e di intervenire prima che sia troppo tardi -

[200] R. DUIZONI, *Mappatura di aree a rischio e formazione della relativa documentazione dimostrativa dei passi compiuti da offrire al giudice o al pubblico ministero quale attività ex 391-nonies c.p.p. attività investigativa preventiva*, in www.rivista231.it.
[201] R. TREZZA, *I valori giuridici possono mai trasformarsi in variabili algoritmiche?*, cit.
[202] F. LEDDA, *I protocolli dei Modelli Organizzativi*, in www.rivista231.it.

mentre, la fase repressiva necessita dell'intervento del giudice umano[203] che si pronuncerà attraverso un giudizio, non suscettibile di standardizzazione.

Quindi, se da una parte la tecnologia costituisce un ausilio notevole in campo preventivo[204] dall'altro, il giudizio implica l'intervento di un soggetto che possa valutare in concreto i fatti; alla luce di queste preliminari considerazioni sembra che l'introduzione di un modello "matematico 231", completamente automatizzato sia – attualmente – irrealizzabile e che debbano essere incentivate forme di "collaborazione" tra intelligenza artificiale ed umana.

2. *Blockchain* e *criminal compliance*.

La c.d. quarta rivoluzione industriale ha visto lo sviluppo della *blockchain* non solo in ambito finanziario, ma come strumento utile in molti altri settori. Le aziende possono trarre benefici non solo a livello di tempistiche di lavorazione dei processi, ma soprattutto in termini di trasparenza e di disintermediazione delle transazioni con una forte riduzione dei costi di gestione.

L'impiego della *blockchain* porta con sé anche dei lati oscuri e dei rischi in quanto può costituire il mezzo attraverso il quale commettere reati; ad esempio, frodi, riciclaggio, spionaggio industriale.

---

[203] In questo senso R. TREZZA, *L'intelligenza artificiale come ausilio alla standardizzazione del modello*, cit.

[204] R. TREZZA, *I "valori giuridici" possono mai trasformarsi in variabili algoritmiche?*, cit.

Per bilanciare i vantaggi ed i rischi delle DLT è necessario dotarsi di un'idonea regolamentazione e – come si vedrà nel prossimo capitolo – sembrerebbe che in ambito europeo il legislatore si stia muovendo in questa direzione.

La *blockchain* ha delle ripercussioni sulla *compliance* in generale, ma per quanto riguarda la prevenzione dei reati di cui al d.lgs. 231 del 2001, l'impiego della tecnologia in oggetto potrebbe determinare il superamento di alcune forme di reato e di conseguenza la riscrittura dei modelli organizzativi.

I reati che potrebbero essere disincentivati dall'impiego della tecnologia *blockchain* sono ad esempio, quelli che implicano l'utilizzo di somme di denaro si pensi, ai reati contro la pubblica amministrazione: peculato, corruzione, concussione, malversazione ai danni dello stato e così via.

In questi casi il fatto che la *blockchain* permetta la tracciabilità di ogni transazione potrebbe costituire un deterrente per i trasferimenti di denaro illegali in quanto, l'utilizzo della crittografia asimmetrica consentirebbe di risalire, in maniera univoca, al destinatario ed al mittente della somma di denaro.

La *blockchain* potrebbe essere impiegata anche, nei delitti contro l'incolumità pubblica[205] ed operare come strumento di verifica del prodotto, consentendo al consumatore di tracciare la filiera produttiva e la qualità della merce.

[205] Si pensi ai reati di: adulterazione o contraffazione di sostanze alimentari (art. 440 c.p.), commercio di sostanze alimentari contraffatte o adulterate (art. 442 c.p.), contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517-quater).

Sono molti altri i settori in cui si potrebbe utilizzare la tecnologia a registro distribuito per prevenire la realizzazione di condotte illecite, ma ciò implica un necessario ripensamento delle attività da parte delle aziende nell'ottica della quasi totale automatizzazione dei processi e delle tecniche preventive.

2.1 L'analisi dei flussi informativi.

L'intelligenza artificiale intesa come metodo che consente di estrarre ed elaborare informazioni da una grande quantità di dati al fine di svolgere plurime operazioni anche di carattere predittivo.

Nella realtà aziendale vengono utilizzati in maniera crescente gli strumenti dotati della capacità di autoapprendimento, di migliorare e di modificare le prestazioni sulla base dell'esperienza[206].

La risorsa su cui si basa il funzionamento dell'Intelligenza artificiale sono i dati che possono essere elaborati in vari modi; in primo luogo, si può avere un apprendimento supervisionato, il quale prevede un intervento umano perché i dati con cui il sistema viene pensato sono selezionati e categorizzati; in secondo luogo, si parla di un apprendimento non supervisionato quando i dati sono raggruppati dal sistema stesso senza previa "istruzione" da parte dell'agente umano[207].

---

[206] J. DREXL, R.M. HILTY ET AL., *Technical Aspects of Artificial Intelligence: An Understanding from an Intellectual Property Law Perspective*, Version 1.0, ottobre 2019, 8.

[207] K. WALCH, *Is there a Difference between Assisted Intelligence vs. Augmented Intelligence?*, in Forbes, 12 gennaio 2020; Y. RUI, *From Artificial Intelligence to Augmented Intelligence*, in *IEEE MultiMedia*, gennaio 2017, vol. 24, n. 1, p. 4 ss.

L'IA in ambito aziendale viene impiegata per assistere il *board* nell'analisi dei flussi informativi, in quanto garantisce una maggiore precisone nella ricerca e nell'analisi dei dati, ma soprattutto velocizza i tempi di lavorazione[208].

Il sistema automatizzato può essere utilizzato in funzione di supporto alle decisioni, ma presenta anche dei rischi; in particolare si fa riferimento all'assenza di *accountability* e all'impossibilità di contestare le decisioni adottate[209].

Il meccanismo c.d. *black box* contribuisce a rendere il sistema "opaco", ciò è frutto soprattutto della complessità degli algoritmi impiegati e della capacità di questi di autoapprendere.

L'impossibilità di prevedere *ex ante* il risultato che l'IA potrebbe fornire insieme all'assenza di trasparenza che è connaturata negli algoritmi – spesso avvolti dalla tutela della proprietà intellettuale – sono determinanti in termini di conoscibilità e di *explinability*.

L'impresa per una corretta gestione delle attività deve garantire la trasparenza non solo dei flussi informativi, ma anche degli algoritmi impiegati; i due livelli si intersecano e se correttamente "maneggiati" rendono le decisioni prese controllabili e di conseguenza l'organo collegiale *accountable*.

---

[208] G.D. MOSCO, *Roboboard. L'intelligenza artificiale nei consigli di amministrazione*, in *Riviste Web*, 247-260.

[209] M. LILLÀ MONTAGNANI, *Flussi informativi e doveri degli amministratori di società per azioni ai tempi dell'intelligenza artificiale*, in *Riv. Persona e mercato*, 2, 2020.

I sistemi di IA modificano il modo di adottare le decisioni e obbligano le imprese a dotarsi di soggetti esperti che possano aiutare gli organi a capire come funzionino gli algoritmi adottati.

Invero, sono molti i tipi di figure emergenti in ambito aziendale sia a livello privato che pubblico che assumono il compito di spiegare il funzionamento degli algoritmi e di risolvere gli eventuali problemi tecnici che si presentino durante l'utilizzo dei sistemi: si pensi ai comitati[210] che hanno la funzione di garantire la sicurezza informatica e di supervisionare i sistemi di IA; oppure, nel caso non si voglia o non si possa istituire un comitato *ad hoc* potrebbero essere ampliate le funzioni di quelli già esistenti in ambito informatico al pari di quanto accade per il responsabile della protezione dati[211]; ancora, si può pensare di istituire un *algorithm officer*[212] con il compito di valutare la trasparenza degli algoritmi impiegati.

Si può dire che lo sviluppo delle nuove tecnologie richiede uno sforzo sempre più pregnante in termini di controllo e di prevenzione del rischio dovuto principalmente alle potenzialità degli algoritmi che sono sempre più avanzati e capaci di autoapprendere e di conseguenza pongono problemi di *explinability* e di assenza di trasparenza; le imprese sicuramente hanno la

[210] L.A. ENRIQUES - D.A. ZETZSCHE, *Corporate technologies and the Tech Nirvana Fallacy*, 2019, 19.

[211] M. LILLÀ MONTAGNANI, *Flussi informativi e doveri degli amministratori di società per azioni ai tempi dell'intelligenza artificiale*, cit., 103 ss.

[212] C. THIBAULT, *Why your company needs a Chief Algorithms Officer*, 26 settembre 2018.

possibilità di sfruttare le caratteristiche positive dei nuovi sistemi, ma allo stesso tempo, devono adoperarsi e gestirli in maniera *compliant*.

2.2 L'impiego dei DLT e delle criptovalute nei processi finanziari aziendali.

Le tecnologie a registro distribuito – nello specifico la *blockchain* – come si è visto, utilizzano una rete *peer-to-peer* che consente di raggiungere il consenso senza doversi affidare ad intermediari e ad un ente centralizzato per la gestione delle informazioni e dei dati verso i soggetti esterni all'azienda.

L'impiego dei DLT consente di implementare l'accessibilità dei dati e di verificare in tempo reale tutte le informazioni accrescendo la trasparenza della azienda e la fiducia da parte degli *stakeholders*.

L'automatizzazione delle procedure elimina i costi di transazione sia per l'impresa che per gli utenti, in quanto, gli intermediari vengono sostituiti dal meccanismo di validazione su cui si basa la *blockchain* (consenso distribuito sui nodi della catena).

La riduzione dei costi di intermediazione però, viene compensata dalla necessità di affrontare nuove spese; ad esempio, quelle relative ai *miner* che vengono remunerati in *token* o criptovalute; tali costi però sono sicuramente più vantaggiosi e proficui per l'impresa date le semplificazioni che consentono di conseguire.

L'utilizzo dei sistemi a registro distribuito nei processi finanziari ha avuto un rapido sviluppo soprattutto per la diffusione delle criptovalute che non necessitano di intermediazione per lo scambio, non si basano su un supporto fisico e vengono accettate in tutto il mondo; allo stesso tempo, però, sono caratterizzate da una forte volatilità che rende instabile il loro potere d'acquisto e quindi ne limita la diffusione.

Il rischio maggiore per le imprese derivante dall'impiego di valute virtuali risiede nel riciclaggio di "denaro sporco"[213].

Quando si parla di criptovalute generalmente si pensa ai *bitcoin*; a tal proposito, si deve considerare che nel tempo si sono diffuse altre tipologie di valute virtuali che rientrano nella categoria degli Alt Coin.

Alla base delle valute virtuali risiede un meccanismo *peer to peer* (da pari a pari) in cui ciascun nodo può fare sia da *client* che da *server*[214].

[213] Per un approfondimento sul tema, tra gli altri: U. BECHINI – M. C. CIGNARELLA, *Antiriciclaggio – compravendita di immobile – pagamento del prezzo in bitcoin, Quesito antiriciclaggio n. 3/2018*, in Not., 20 marzo 2018; A. CAPOGNA - L. PERAINO - S. PERUGI - M. CECILI - G. ZBROWSKI - A. RUFFO, *Bitcoin: profili giuridici e comparatistici. Analisi e sviluppi futuri di un fenomeno in evoluzione*, in *Di.m.t*., 2015, in nota 23; G. GASPARRI, *Timidi tentativi giuridici di messa a fuoco del Bitcoin: miraggio monetario criptoanarchico o soluzione tecnologica in cerca di un problema?*, in *Dir. Inform.*, 2015, 415 ss.; P. IELO, *Autoriciclaggio e responsabilità dell'ente ex d.lgs. 231/2001*, in MEZZETTI - PIVA, *Punire l'autoriciclaggio. Come, quando e perché*, Torino, 2016, 50 ss.; G. MOLINARO, *Sono tassabili le manifestazioni di capacità economica emergenti nelle operazioni relative al bitcoin*?, in *Corr. Trib*., 2018, 2447; P. M. SABELLA, *Vendita di società "ready made" ed obblighi di verifica della clientela nella disciplina sulla prevenzione di riciclaggio e finanziamento del terrorismo: contrasto all'anonimato e valute virtuali*. Nota a CGUE Grande sezione 17 gennaio 2018 (causa C.676/16), in DPCE online, 2018, 2, 545 ss.

[214] S. CAPACCIOLI, *Criptovalute e bitcoin. Un'analisi giuridica*, Milano, 2015, 21; M. ATZORI, *Blockchain Technology and Decentralized Governance Is the State Still Necessary?*, in *Ssrn.com*, 2 gennaio 2016.

L'acquisto dei beni tramite detta tecnologia avviene in anonimato e questo accentua il rischio che le operazioni siano commesse al fine di "ripulire" denaro.

Le valute virtuali vengono scambiate attraverso la rete che per le sue particolari caratteristiche rappresenta il luogo ideale per la commissione di attività illecite: si pensi alla delocalizzazione (che determina difficoltà nell'individuazione del *locus commissi delicti*), alla dispersione che rende complessa l'identificazione dell'illecito, alla dematerializzazione non solo del denaro, ma anche dei servizi e delle informazioni.

Orbene, essendo queste le premesse si può ben capire come le criptovalute assumano un ruolo fondamentale nell'ostacolo all'identificazione della provenienza illecita della ricchezza[215].

Invero, la tecnologia DLT è caratterizzata da trasparenza, parziale immutabilità e irrepudiabilità, in quanto si basa sulla crittografia asimmetrica che attraverso l'utilizzo di chiavi pubbliche e private consente la protezione e l'autenticazione delle transazioni, ma qualora venga adoperata allo scopo di impedire la tracciabilità del denaro, dei beni o di altre utilità rappresenta uno strumento mediante il quale commettere i reati di riciclaggio e reimpiego di valute virtuali.

[215] G.J. SICIGNANO, *L'interesse e il vantaggio dell'ente nel riciclaggio mediante criptovalute,* in *Riv. 231*, 2021.

La normativa a livello sia europeo che nazionale ha preso atto del rischio ed ha implementato la disciplina in materia di riciclaggio ed autoriciclaggio[216], adeguando anche il decreto relativo alla responsabilità da reato della persona giuridica, introducendo l'articolo 25-octies1[217] che disciplina i delitti in materia di strumenti di pagamento diversi dai contanti.

A questo punto, però, ci si è chiesti quali siano i criteri di ascrizione della responsabilità della persona giuridica in caso di condotte di riciclaggio mediante criptovalute.

Il d.lgs. 231 del 2001 per ritenere responsabile la persona giuridica richiede la prova che la persona fisica abbia agito al fine di realizzare un interesse o vantaggio per l'ente.

Per quanto riguarda l'interesse perché si possa muovere un rimprovero nei confronti della persona giuridica è necessario che l'agente abbia acquistato criptovalute per realizzare un'operazione societaria e non per scopi personali. La prova risulta essere molto complessa in quanto l'anonimato che caratterizza le DLT rende difficile identificare il proprietario del portafoglio e di conseguenza il collegamento tra l'operazione e l'ente. Discorso analogo vale per la prova del vantaggio.

[216] La Direttiva UE 2019/713, prevede l'incriminazione di condotte che utilizzino le criptovalute per finalità illecite; il D.lgs. 8 novembre 2021, n. 184, prevede l'incriminazione di condotte che vedano l'utilizzo di strumenti di pagamento diversi dal contante per finalità illecite.

[217] Articolo introdotto dalla legge 3 agosto 2009, n. 116 e sostituito dal D.lgs. 7 luglio 2011, n. 121.

Quest'ultimo ha carattere oggettivo e viene in rilievo, ad esempio, quando il soggetto agente abbia acquistato per un interesse meramente personale, ma all'ente derivi un guadagno speculativo.

In questo caso si può configurare un vantaggio per la persona giuridica?

Si è osservato che la risposta sembra essere negativa[218], derivandone per l'ente un mero vantaggio fortuito e non corrispondente alla sua volontà.

Nonostante le difficoltà che si possono riscontrare in ordine alla prova dell'interesse o vantaggio, osserva parte della dottrina, che la possibilità per l'ente di andare esente da responsabilità in caso di riciclaggio mediante criptovalute sia davvero esigua; questo in primo luogo, per la difficoltà di riconoscere l'idoneità del modello ed in secondo luogo, per il meccanismo presuntivo che avvolge l'equazione cripto-valuta/cripto-attività che conferisce automaticamente carattere illecito alle operazioni che adoperano moneta virtuale.

Alla luce delle suddette considerazioni si può rilevare che le potenzialità delle criptovalute e della *blockchain* per le imprese sono molte, ma per poter essere sfruttate al meglio necessitano di una completa regolamentazione che consenta alle aziende di conciliare benefici della tecnologia con la *compliance* richiesta a livello normativo.

[218] G.J. SICIGNANO, *L'interesse e il vantaggio dell'ente nel riciclaggio mediante criptovalute*, cit., 109 ss.

3. L'utilizzo di sistemi automatizzati nella fase di *risk assesment* e di *risk management*.

Gli strumenti tecnologici sono un valido strumento sia nella fase di ricognizione e valutazione del rischio che nella fase di gestione dello stesso.

La costruzione del modello organizzativo vede il susseguirsi di varie fasi; la prima consiste nella mappatura dell'azienda e nella trasformazione dei dati in forma numerica per poterli elaborare e correlare tra loro.

La tecnologia in una prima fase serve ad analizzare la realtà aziendale fornendo un'immagine realistica[219] del modo d'essere della stessa che consenta a posteriori di valutare l'idoneità del modello organizzativo rispetto all'architettura che assume l'azienda.

Nella fase di progettazione del modello gli strumenti digitali vengono impiegati per la prevenzione del rischio in quanto, consentono di monitorare e controllare i processi interni e di procedimentalizzare le attività in conformità alle regole normative vigenti ed in costante aggiornamento.

L'utilizzo di algoritmi favorisce anche la fase di aggiornamento della normativa data la sua caratteristica di continua evoluzione che implica il repentino apporto di modifiche al modello organizzativo.

La gestione del rischio si estrinseca in una corretta predisposizione del modello, ma soprattutto nella sua efficace attuazione; lo strumento digitale

[219] A. GARAPON-LASSAGUE, *La giustizia digitale*, Bologna, 2021, 111-112; R. BODEI, *Dominio e sottomissione*, Bologna, 2023, 333.

supporta la realizzazione dell'effettività e dell'efficacia del *compliance program*[220].

La tecnologia consente di monitorare e rilevare in tempo reale gli eventuali segnali d'allarme e le potenziali violazioni del modello[221]; ad esempio, nel caso di reati che prevedano la possibilità di codificare in termini numerici la conformità o non conformità normativa, l'utilizzo di sistemi di monitoraggio automatico facilita la rilevazione del rischio e la conseguente prevenzione dell'illecito[222].

Si pensi ai reati di riciclaggio, corruzione, ma anche agli illeciti in materia ambientale oppure relativi ai mercati finanziari[223] che potrebbero supportare o addirittura sostituirsi al controllo interno effettuato in forma manuale ed analogica.

Inoltre, la procedimentalizzazione in forma digitale ed automatizzata delle attività aziendali consente il tracciamento costante delle operazioni, dei flussi

---

[220] C. BURCHARD, *Digital criminal compliance*, in *Digitalisierung, Globalisierung und Risikoprävention. Ferschrift für Ulrich Sieber zum 70. Geburstag*, a cura di Engelhart – Kudlich – Vogel, Berlin, 2021, 744.

[221] G. MORGANTE, G. FIORINELLI, *Promesse e rischi della compliance penale digitalizzata*, in *Archivio penale*, 2022, 10 ss.

[222] S. SHETTY - M. MUSA - X. BRÈDART, *Bankrupctcy prediction Using Machine Learning Techniques*, in *Journal of Risk and Financial Management*, 15, 35, 1-10.

[223] Sul tema della prevenzione dei reati mediante l'intelligenza artificiale si vedano tra gli altri: E. BIRRITTERI, *Big Data Analytics e compliance anticorruzione. Profili problematici delle attuali prassi applicative e scenari futuri*, in *Dir. Pen. Cont*., 2019, 2, 289-303; R. SABIA, *Artificial Intelligence and Enviromental Criminal Compliance*, in *Revue Internationale de Droit Pènal*, 2020, 179-201; F. CONSULICH, *Il nastro di Mobius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso di mercato*, in *Banca borsa titoli di credito*, 2018, 2, 195-234; TCW LIN, *Compliance, technology, and modern finance*, in *Brooklin Journal of Corporate, Financial and Commercial Law*, 2016, 11, 159-182.

informativi, ma anche delle eventuali segnalazioni, facilitando la prova in giudizio dell'attuazione del modello; in altre parole, ciò determina un preciso tracciamento del monitoraggio realizzato con una conseguente misurazione della correttezza del sistema di *compliance*[224].

L'uso della tecnologia potrebbe determinare una prevenzione diretta dei reati; infatti, nel momento in cui i processi ed i protocolli saranno automatizzati e programmati per agire entro determinati *standard* la realizzazione dell'illecito non dipenderà più dalla volontà diretta del destinatario della regola essendo l'operazione impedita automaticamente dal sistema.

Orbene, le potenzialità della tecnologia rispetto alla predisposizione ed all'implementazione del modello sono plurime e consentirebbero di garantire l'efficacia e l'efficienza del modello però, è necessario considerare anche i rischi che tale automatizzazione porta con sé in termini di utilizzo dei dati personali e di realizzazione di forme di sorveglianza rispetto ai soggetti che operano in azienda.

4. Gli obblighi imposti dalla normativa a tutela della privacy.

L'intelligenza artificiale e lo sviluppo tecnologico hanno reso il tema della *data protection* sempre più centrale; infatti, i dati oltre ad essere

[224] Sul punto: D. C. LANGEVOORT, *Global Behavioral Compliance*, in *Corporate on a Global Scale, in Corporate Compliance on a Global Scale*, 2022, 217-236., 217.

innumerevoli, spesso vengono utilizzati per finalità che vanno oltre i limiti del consenso prestato dal titolare.

Quando si parla di *privacy* ci si riferisce ad una pluralità di concetti che hanno in comune il bene giuridico tutelato.

L'opinione prevalente[225] ritiene che la *privacy* si componga del diritto alla riservatezza e alla tutela della vita privata e che il fondamento costituzionale sia da riferire all'articolo 2 della Costituzione che tutela i diritti inviolabili dell'individuo.

A livello europeo il Regolamento n. 679 del 2016[226] ha riconosciuto tutela universale alla protezione dei dati personali con diritti uniformi per tutti i cittadini europei.

Il GDPR si proponeva di accrescere il livello di consapevolezza riguardo all'utilizzo dei dati da parte dei titolari del trattamento introducendo il principio di *accountability*, che grava principalmente sul Responsabile[227].

Il Regolamento per garantire una protezione dei dati più pervasiva disciplina la *data protection by design e by default* con l'obiettivo ultimo di minimizzare il trattamento dei dati, utilizzandoli solo per le finalità necessarie e nel rispetto del consenso prestato.

---

[225] Tra gli altri: F. MANTOVANI, *Diritto alla riservatezza e libera manifestazione del pensiero*, Milano, 1970, 29 ss.

[226] L. BOLOGNINI – E. PELINO – C. BISTOLFI, *Il regolamento privacy europeo*, Milano, 2018.

[227] A. MANTELERO, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva*, in G. FINOCCHIARO, (a cura di) *Il nuovo Regolamento Europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017.

A livello aziendale viene introdotta la figura del *data protection officer* (DPO) che ha assunto compiti di monitoraggio e controllo[228].

Il quadro normativo risulta essere in costante aggiornamento anche alla luce dell'avvento delle nuove tecnologie che hanno imposto un ripensamento del contenuto del diritto alla *privacy*, con una corretta diffusione e gestione dei dati.

La *privacy* intesa come *right to let be alone*, vede mutare il suo contenuto da diritto alla riservatezza a diritto all'autodeterminazione informativa[229].

Il privato non ha più il mero interesse alla tutela esclusiva dei dati, ma il diritto alla riservatezza viene proiettato nella sua dimensione sociale ed inteso quale corretto controllo delle informazioni che lo riguardano.

Alla luce del quadro normativo europeo e nazionale in materia di *privacy* sarà necessario capire in che modo conciliare la *criminal compliance* con la tutela dei dati.

5. Come conciliare la *digital criminal compliance* con la tutela dei diritti dei soggetti coinvolti dall'analisi dei dati?

L'innovazione tecnologica ha un forte impatto sul diritto alla *privacy* proprio perché la macchina tecnologica si basa essenzialmente sui dati.

---

[228] A. AVITABILE, *Il data protection officer*, in G. FINOCCHIARO, (a cura di) *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, 2017.

[229] L. D'AGOSTINO, *La tutela penale dei dati personali nel riformato quadro normativo: un primo commento al D.Lgs. 10 agosto 2018, n. 101*, in *Archivio pena*le, 2018, 1-58; A. BALDASSARRE, *Diritti della persona e valori costituzionali*, Torino, 1997, 57 ss.

La *blockchain* – come si è visto – rappresenta un'opportunità in termini di maggiore trasparenza e disintermediazione però, può in concreto avere dei riflessi negativi rispetto alla tutela dei dati personali.

In primo luogo, la replica delle informazioni sui vari nodi contrasta con il principio di minimizzazione dei dati, che disciplina un utilizzo adeguato, pertinente e limitato rispetto alla finalità del trattamento.

In secondo luogo, la *blockchain* basandosi sulla pseudoanonimizzazione consente di risalire al titolare degli stessi anche se criptati, questa caratteristica se da un lato consente di individuare attività illecite dall'altro rischia di confliggere con la liceità del trattamento[230].

Sulla stessa linea anche l'utilizzo dell'intelligenza artificiale può rappresentare un rischio per la *privacy.* Nello specifico nell'analisi dei dati risulta difficile rispettare la finalità del trattamento[231].

Il principio di esattezza dei dati e di aggiornamento, quello di minimizzazione e adeguatezza, vietano di reperire i dati come se si eseguisse un "pesca a strascico"[232] senza avere chiari gli scopi perseguiti e non considerando la correttezza e l'esattezza dei dati utilizzati.

---

[230] N. FABIANO, *The Internet of Things ecosystem: the blockchain and privacy issues. The challenge for a global privacy standard Advances*, in *Science, Technology and Enginnering Systems Journal*, vol. 3, n. 2, 2018, 5.

[231] G. PITRUZZELLA, *Big data, competition and privacy: a look from the antitrust perspective, concorrenza e mercato*, 2016, 15-20.

[232] F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, 2018, Torino.

Quindi le imprese devono poter utilizzare i sistemi di IA senza rischiare di incorrere in responsabilità per lo scorretto utilizzo e trattamento dei dati; la strada è ancora lunga, ma si può dire che in tal senso sono stati fatti notevoli passi avanti.

6. La possibile automatizzazione delle investigazioni interne: problemi e prospettive.

La responsabilizzazione della persona giuridica e l'implementazione di obblighi di *compliance* sempre più pregnanti suggeriscono di agire anticipatamente rispetto all'autorità giudiziaria nel caso in cui si abbia il sospetto oppure si verifichi un rischio di tipo civile, amministrativo, penale o anche solo reputazionale; a tal fine, sempre più frequentemente le imprese ricorrono allo strumento dell'investigazione interna, allo scopo di rilevare potenziali violazioni di legge o delle *policy* aziendali.

Sebbene l'istituto abbia una forte potenzialità – soprattutto nell'ottica di promuovere la collaborazione pubblico-privato e di incentivare forme di giustizia riparativa – l'abbondanza di norme e l'incertezza giurisprudenziale non permette di poter fruire a pieno delle potenzialità dello strumento[233].

[233] C. APPETITI, *Il sistema di compliance di UniCredit*, in ROSSI, *La corporate compliance: una nuova frontiera per il diritto?*, Milano, 2017, 51; M. MANTOVANI – L. FRANCESCHINI, *La compliance in ENI*, in *La corporate compliance: una nuova frontiera per il diritto?*, Milano, 2017, 1; E. M. MANCUSO, *L'acquisizione di contenuti e-mail*, in SCALFATI, *Le indagini atipiche*, Torino, 2014, 256; N. BOURTIN - A. HOULE, *Investigazioni interne: uno sguardo all'esperienza americana*, in CENTONZE – MANTOVANI, *La responsabilità penale degli enti: dieci proposte di riforma*, Bologna 2016, 199.

Orbene - dopo aver delineato le caratteristiche principali delle investigazioni interne - si cercherà di capire quali sono le possibili applicazioni delle nuove tecnologie a tale istituto.

L'ente può decidere di avviare un'investigazione interna in seguito alla ricezione di una segnalazione proveniente da varie tipologie di fonti[234], al fine di adottare dei rimedi proficui e strutturare un'idonea difesa.

La finalità può essere interna oppure esterna; nel primo caso[235], è volta a verificare la tenuta del modello organizzativo oppure alla decisione di avviare un procedimento disciplinare a carico di apicali o sottoposti, mentre nel secondo[236], in vista di un procedimento in corso o futuro, mira ad acquisire una conoscenza delle informazioni utili alla ricostruzione dei fatti oggetto di indagine da parte dell'autorità giudiziaria ed a predisporre un'adeguata strategia difensiva.

Dell'indagine interna viene investito un polo investigativo[237] costituito di volta in volta sulla base dell'oggetto investigativo da esperti di materia appartenenti alle funzioni legali, di *internal audit* e di *compliance*.

---

[234] G. DI GARBO – F. GAUDINO – E. M. MANCUSO – M. VASILE, *Italy*, in SPEHL – GRUETZNER, *Corporate internal investigation*, München, 2012, 248.

[235] E. M. MANCUSO, *Le investigazioni interne nel procedimento a carico dell'ente*, in D. CASTRONOVO – G. DE SIMONE – E. GINEVRA – A. LIONZO – D. NEGRI – G. VARRASO, *Compliance. Responsabilità da reato degli enti collettivi,* 2019, 1935 ss.

[236] A. NIETO MARTÌN, *Internal investigation, Whistle-Blowing, and Cooperation: The Struggle for Information in the Criminal Process*, in MANACORDA – CENTONZE – FORTI, *Preventing corporate corruption. The Anti-Birbery Compliance Model*, Cham-Heidelberg, 2014, 69; M. PANASITI, *sub. Art. 17*, in LEVIS-PERINI, *La responsabilità amministrativa delle società e degli enti*, Bologna, 2014, 356.

[237] BARRY F. MCNEIL – D. BRAIN, *Internal Corporate Investigations*, Chicago, 2007, 11.

Insieme ai componenti interni alla società collaborano spesso anche soggetti esterni esperti in indagini contabili o forensi, per gli aspetti che presentano maggiori criticità e tecnicismi.

Acquisisce un ruolo fondamentale nell'ambito delle investigazioni interne l'organismo di vigilanza[238], che ha la possibilità di individuare e gestire i flussi informativi in modo da rilevare le potenziali violazioni e gli illeciti commessi da parte dei dipendenti della società.

L'attività investigativa parte da una completa analisi documentale ed in questa fase l'impiego della tecnologia potrebbe incrementare la velocità e la completezza delle informazioni acquisite.

La documentazione spesso è detenuta dai dipendenti della società[239] e l'investigatore, sia interno che esterno, sebbene abbia ampio accesso ai contenuti in alcuni casi potrebbe non esserci stata un'adeguata separazione dei *file* personali da quelli attinenti all'attività di lavoro, con conseguente difficoltà nel reperimento della fonte di prova nel rispetto della normativa in materia di tutela dei dati personali[240].

Allo stesso tempo, l'indagine relativa alla posta elettronica può risultare complessa perché in molti casi è difficile da scorporare il contenuto dei

[238] E. M. MANCUSO, *Le investigazioni interne nel procedimento a carico dell'ente*, cit., 1937 ss.

[239] P. VENTURA, *Le indagini difensive*, in UBERTIS-VOENA, *Trattato di procedura penale*, Milano, 2005, XXVII, 2, 124.

[240]E. M. MANCUSO, *Le investigazioni interne nel sistema processuale italiano: tra vuoto normativo e prassi applicative incerte*, in CENTONZE-MANTOVANI, *La responsabilità penale degli enti: dieci proposte di riforma*, Bologna, 2016, 217.

messaggi a carattere lavorativo da quello di tipo privato. L'utilizzo dell'intelligenza artificiale potrebbe aiutare nell'analisi della documentazione in quanto basandosi su algoritmi spesso capaci di individuare "parole chiave" che potrebbero classificare a priori il messaggio come personale oppure attinente all'attività lavorativa.

L'analisi dei flussi informatici e l'impiego di tecniche di intelligenza artificiale per un capillare e generalizzato controllo pone il problema del rispetto della disciplina in materia di controllo dei lavoratori e di tutela dei dati e del domicilio informatico[241] dei soggetti coinvolti.

A livello europeo, l'articolo 22 del Regolamento in materia di protezione dei dati personali e l'articolo 11 della Direttiva 2016/680/UE sulla protezione dei dati personali nell'attività di prevenzione, indagine, accertamento e perseguimento dei reati vietano l'adozione di decisioni basate esclusivamente su trattamenti automatizzati, essendo necessario l'intervento umano nell'attività di formazione della volontà[242].

Quindi, si può dedurre che alla luce della delicatezza degli interessi coinvolti il trattamento dei dati non può essere completamente automatizzato, ma si rende necessario il controllo di un soggetto umano che possa effettuare una completa attività valutativa.

---

[241] In tal senso si veda: E. BIRRITTERI, *Big Data Analytics e compliance anticorruzione. Profili problematici delle attuali prassi applicative e scenari futuri*, cit., 295 ss.

[242] L. D'AGOSTINO, *La tutela penale dei dati personali nel riformato quadro normativo: un primo commento al D.Lgs. 10 agosto 2018, n. 101*, in *Archivio Penale*, 2, 2019, 17 ss.

La disciplina delle indagini interne al momento è priva di codificazione, ma per lo svolgimento delle *internal investigation* si possono in parte seguire le norme previste in materia di investigazioni difensive al libro V, titolo VI-bis c.p.p.

In ogni caso le informazioni raccolte possono essere considerate degli elementi di prova in sede processuale, ma saranno sottoposte ad un diverso regime di utilizzabilità a seconda che si tratti di un'investigazione interna indipendente attivata spontaneamente oppure si tratti di una vera e propria indagine difensiva.

Nel primo caso[243] al pari di ogni altra prova documentale sarà liberamente apprezzabile dal giudice ai sensi dell'articolo 234 c.p.p.; nel secondo caso[244], l'ingresso in sede processuale sarà molto più pregnante, ad esempio, i verbali delle audizioni difensive saranno inseriti nel fascicolo del difensore oppure l'oggetto dell'accertamento tecnico non ripetibile (si pensi a quello eseguito su supporti informatici) sarà utilizzabile a livello processuale una volta instaurato il contraddittorio con la parte pubblica, insomma in questo caso sono presenti molti più vincoli da rispettare nell'ottica processuale.

L'avvio di un'indagine difensiva potrebbe essere incentivato dal riconoscimento di benefici premiali; l'atteggiamento collaborativo dell'ente incide sul trattamento sanzionatorio ai sensi dell'articolo 12 del d.lgs.

---

[243] S. CAMPANELLA, *Profili problematici in tema di documenti dichiarativi*, IP, 2008, 162; P. TONINI, *Il valore probatorio dei documenti contenenti dichiarazioni scritte*, CP, 1990, 2219.

[244] P. VENTURA, *Le indagini difensive*, cit., 2; O. MAZZA, *Fascicolo del difensore e utilizzabilità delle indagini difensive*, in *Giur. It.*, 2002, 1758.

231/2001 e in termini di condotte riparatorie ex articolo 17 d.lgs. 231/2001[245]; infatti, si è osservato[246] che la persona giuridica attraverso un atteggiamento proattivo mette a disposizione degli elementi utili a dimostrare la responsabilità per l'illecito verificatosi determinando una cesura con il difetto di una adeguata organizzazione che aveva reso possibile la verificazione della condotta inosservante.

In letteratura[247] sono state avanzate varie proposte di riforma volte a premiare da un punto di vista processuale[248] l'atteggiamento collaborativo dell'ente incentivando forme di non punibilità che siano condizionate alla risoluzione del *decifit* organizzativo.

Invero, incentivare un'autocorrezione dei comportamenti e delle pratiche illecite sembra essere lo strumento più adatto a ristabilire una *compliance* che non sia solo temporanea, ma che possa durare nel tempo; in ogni caso, la tecnologia potrà dare un forte impulso in questo senso sebbene necessiterà di

---

[245] G. VARRASO, *Il procedimento per gli illeciti amministrativi dipendenti da reato*, in UBERTIS-VOENA, *Trattato di procedura penale*, Milano 2012, XLVII, 92.

[246] F. STELLA, *Criminalità d'impresa: lotta di sumo e lotta di judo*, cit., 462.

[247] Tra gli altri: F. CENTONZE – M. MANTOVANI, *La responsabilità penale degli enti: dieci proposte di riforma*, Bologna, 2016, 288; G. FIDELBO – R. A. RUGGIERO, *Procedimento a carico degli enti e messa alla prova: un possibile itinerario*, www.rivista231.it, 2016, 14; E. M. MANCUSO, *L'acquisizione di contenuti e-mail*, cit., 17.

[248] Questo filone dottrinale ipotizza forme di *restorative justice* che vadano oltre il riconoscimento di uno sconto di pena avvicinandosi a forme di non punibilità subordinate alla risoluzione del *deficit* organizzativo. È stato osservato che incentivare forme di giustizia collaborativa facilita l'emersione di condotte riconducibili alla c.d. criminalità d'impresa (ad esempio, a livello internazionale si è rilevato che circa un terzo dei procedimenti per corruzione sorge a seguito della segnalazione dell'impresa coinvolta, in tal senso M. MANTOVANI, *Il d.lgs. n. 231/2001 e gli incentivi alla persona giuridica: il punto di vista dell'impresa*, cit., 117 ss.). Per un approfondimento delle varie proposte di riforma si veda: E. M. MANCUSO, *Le investigazioni interne nel sistema processuale italiano: tra vuoto normativo e prassi applicative incerte*, cit., 1944.

un'idonea regolamentazione volta a contemperare gli interessi dei vari soggetti coinvolti.

7. Un approccio casistico.

Le sfaccettature delle nuove tecnologie – come si è visto – sono molte e rappresentano per il giurista un florido terreno di indagine, in quanto, a fronte delle potenzialità in termini di innovazione e di semplificazione, l'utilizzo della tecnologia comporta plurimi rischi.

Questa parte del lavoro sarà dedicata ad un approfondimento della casistica, prendendo in considerazione le problematiche concernenti, principalmente, il settore bancario in cui le nuove tecnologie hanno avuto un più rapido sviluppo.

Si partirà da casi pratici analizzando il problema prima da un punto di vista tecnico per poi valutare il tipo di illecito che potrebbe verificarsi e la soluzione tecnologica ipotizzata[249].

- Caso 1[250].

[249] Questa parte del lavoro è frutto del periodo di studio effettuato presso l'azienda Cy4Gate, che ha consentito un approfondimento delle tematiche da un punto di vista tecnico.

[250] G. COLÒ, *"Anomaly detection for Cyber Security: Time Series Forecasting and Deep Learning",* in *International Journal of Scientific Research in Mathematical and Statistical Sciences*, Vol.7, Issue.1, 2020, 40-52.

Il monitoraggio della sicurezza informatica in ambito aziendale è fondamentale per rilevare eventuali anomalie nei *log* relativi alle applicazioni utilizzate; in particolare nel settore bancario consente di individuare operazioni potenzialmente sospette. Anche una piccola modifica nel comportamento dell'operatore che lavora su queste applicazioni può essere sintomo di attività illecite in corso; si pensi ad esempio, ad un intento operativo sospetto o ad un'esfiltrazione di dati.

- Cenni teorici.

Prima di trattare il problema da un punto di vista pratico - cercando di comprendere quali siano i possibili utilizzi dell'IA in questo ambito - è necessario capire a livello tecnico come operino i sistemi in oggetto.

L'analisi delle operazioni avviene principalmente attraverso l'utilizzo di serie temporali.

Una serie temporale è un insieme di osservazioni, denotate come x_t, registrate in istanti temporali distinti (t). Nell'ambito di questa trattazione, si porrà particolare attenzione alle serie temporali discrete, in cui l'insieme dei tempi delle osservazioni T_0 è costituito da valori discreti. L'aspetto di maggior rilevanza delle serie temporali risiede nella loro capacità di fornire inferenze in relazione alle leggi sottostanti che le governano.

L'analisi di una serie temporale si svolge attraverso la formulazione di un modello probabilistico che rappresenta i dati. Una volta selezionato il

modello, l'identificazione dei parametri e la validità dello stesso nel rappresentare i dati possono contribuire alla comprensione del processo generativo sottostante.

Un modello di serie temporale probabilistico esaustivo per la sequenza di variabili casuali X_1, X_2, ... rappresenterebbe integralmente tutte le distribuzioni congiunte dei vettori casuali X_1, .., Xn, o equivalentemente tutte le probabilità.

Tuttavia, una tale specifica risulta raramente praticabile nell'analisi delle serie temporali, data l'ampia quantità di parametri da stimare. Di solito, ci si limita a calcolare i momenti del primo e del secondo ordine delle distribuzioni congiunte: i valori attesi $E(X_t)$ e i prodotti attesi $E(X_{t+h}, X_t)$, dove t = 1, 2, ..., h = 0, 1, 2, ..., ponendo l'attenzione sulla sequenza X_t che dipende esclusivamente da tali valori.

L'analisi delle serie temporali adotta un approccio generale, effettuando la tracciatura della serie e conducendo verifiche su:

(a) presenza di una tendenza;

(b) componenti stagionali;

(c) possibili cambiamenti improvvisi e significativi nel comportamento;

(d) eventuali osservazioni anomale.

Un altro approccio consiste nell'esprimere la serie in termini di componenti di Fourier[251], che rappresentano onde sinusoidali a varie frequenze.

Per rilevare le anomalie, in primo luogo devono essere previste le serie temporali. Un metodo come ARIMA[252] adatta un singolo modello a ciascuna serie temporale. Quindi è possibile utilizzare il modello per estrapolare la serie temporale nel futuro.

Nelle applicazioni di sicurezza informatica si hanno molte serie temporali simili in un insieme di unità trasversali: serie temporali per il carico del *server,* le richieste di pagine *web*, lo scambio di *byte*, l'accesso alle applicazioni rilevanti. In questi casi, è meglio addestrare un singolo modello congiuntamente su tutte le serie temporali. Al fine di raggiungere questo obiettivo, si coniugano l'approccio classico con le reti neurali.

- Le reti neurali.

A questo punto è necessario introdurre il concetto di rete neurale. È possibile rappresentare una rete neurale con L strati come la composizione di L funzioni f_i: $E \times H_i \rightarrow E_{i+1}$ dove E_i, H_i ed E_{i+1} sono spazi di prodotto interno per ogni i

[251] La serie di Fourier è una rappresentazione di una funzione periodica attraverso la combinazione lineare di funzioni sinusuoidali. La serie prende il nome dal matematico francese Joseph Fourier che studiò per primo le serie infinite in modo sistematico.

[252] I modelli ARIMA (Autoaggressive Integrated Moving Average) sono modelli statistici impiegati per analizzare e prevedere i dati relativi alle serie temporali.

$\in [L]$. Si farà riferimento alle variabili $x_i \in E_i$ come variabili di stato e a $\theta_i \in H_i$ come parametri.

L'*output* di una rete neurale per un *input* generico $x \in E_1$ è una funzione $F: E_1 \times (H_1, ..., H_L) \rightarrow E_{L+1}$ secondo $F(x; \theta) = (f_L \circ ... \circ f_1)(x)$.

L'obiettivo di una rete neurale è ottimizzare una funzione di "loss" J rispetto ai parametri θ su un insieme di n input di rete $D = \{(x(1), y(1)), ...,(x(n), y(n))\}$. dove $x(j) \in E_1$ è il j-esimo punto di *input* con la risposta o l'obiettivo associato $y(j) \in E_{L+1}$. La maggior parte dei metodi di ottimizzazione si basa sui gradienti; quindi, è necessario calcolare il gradiente di J rispetto ai parametri in ogni strato $i \in [L]$.

Per quanto riguarda la funzione di "loss", si utilizzeranno derivate di questa funzione per un singolo punto $(x, y) = (x(j), y(j))$ per qualche $j \in [n]$ e si presenterà poi l'errore di retropropagazione in un formato conciso.

Le funzioni di perdita definiscono la qualità della previsione. La scelta della funzione di perdita deve essere fatta in relazione al problema e ai dati che si vogliono analizzare. Ad esempio, una scelta deve essere fatta quando si decide se la funzione di perdita debba essere simmetrica. Ciò significa che un errore di previsione negativo viene considerato come causa della stessa perdita di un errore positivo dello stesso valore assoluto.

Le differenze tra errori di previsione elevati sono valutate come più importanti rispetto alle differenze tra piccoli errori di previsione.

Una rete neurale è una collezione di neuroni artificiali collegati tra loro. I neuroni sono organizzati in strati. Le reti neurali sono costruite in modo tale

che ogni neurone in uno strato riceva più *input* e produca un singolo *output* (che può essere utilizzato come *input* per altri neuroni). Per introdurre un meccanismo di soglia per attivare il neurone, viene utilizzata una funzione di attivazione (vedere la figura 3 per i diversi tipi di funzione di attivazione).

In una rete multistrato, quando un *input* viene elaborato da un neurone, viene moltiplicato per un valore di peso. Ad esempio, un neurone con 3 *input* ha 3 valori di peso che vengono regolati durante il *training*. Lo spazio dei pesi è l'insieme di tutti i possibili valori degli stessi.

L'algoritmo di retropropagazione cerca il minimo della funzione di errore nello spazio dei pesi utilizzando il metodo della discesa del gradiente. Poiché questo metodo richiede il calcolo del gradiente della funzione di errore ad ogni iterazione, i metodi di apprendimento basati sul gradiente presentano un problema: in alcuni casi, il gradiente sarà piccolo e impedirà al peso di cambiare i suoi valori, il che potrebbe fermare ulteriori addestramenti della rete neurale. Questo è noto come problema del gradiente che scompare. Per affrontare questo problema, introduciamo la rete LSTM (*Long Short-Term Memory*).

Le reti LSTM garantiscono il mantenimento di un errore costante per consentire alla RNN (rete neurale ricorrente) di imparare su intervalli di tempo lunghi, ciò che le permette di associare i problemi e i loro effetti da remoto. Questo è particolarmente utile quando si ha necessità di maggiore "contesto" durante l'analisi. Infatti, le RNN non sono in grado di "imparare" quando aumenta la distanza tra due informazioni.

Il comportamento predefinito delle LSTM è di ricordare le informazioni per lunghi periodi di tempo. Le LSTM hanno la stessa struttura a catena di una RNN, ma invece di avere un singolo strato di rete neurale, ne hanno quattro che interagiscono in modo specifico. Partiamo dallo stato della cella, che è il trasportatore delle informazioni e può essere visto come una linea orizzontale con interazioni lineari minori. Man mano che i dati scorrono all'interno dello stato della cella, la LSTM può aggiungere o rimuovere informazioni e questa azione è regolata da strutture chiamate *gate*. I *gate* rappresentano un modo per far passare le informazioni, con uno strato di rete neurale sigmoidale e un'operazione di moltiplicazione punto per punto. Come già visto, lo strato sigmoidale produce numeri tra zero e uno, descrivendo quanto della componente dovrebbe essere lasciato passare: zero significa blocco delle informazioni, uno significa che tutte le informazioni passano. Una LSTM ha tre *gate* per proteggere e controllare lo stato della cella.
Nel prosieguo si vedrà come applicare i modelli introdotti sopra, nell'ambito delle applicazioni di sicurezza informatica.

- Uso dell'AI.

Al fine di circoscrivere il problema e di poter far funzionare il modello anche su postazioni di lavoro personali, nel modello di *detection* introdotto dall'ipotetica banca X, sono stati considerati gruppi di 10 operatori che lavorano su applicazioni sensibili. La raccolta dei *log* è stata effettuata per 15

giorni e si sono osservate le previsioni del modello giorno per giorno, al fine di individuare anomalie che potessero essere "spia" di attività malevole in corso.

Le serie temporali più importanti riguardavano gli aspetti dell'attività (tutti eseguiti ogni ora e ridotti a valori numerici): operazioni generali effettuate dall'utente, *app* specifiche utilizzate, funzioni specifiche dell'*app* utilizzate, valore restituito dall'*app*.

I modelli introdotti precedentemente venivano utilizzati per prevedere i valori futuri, osservare quanto i valori rilevati ogni ora differivano da quelli previsti e, successivamente, individuare i punti temporali con la massima verosimiglianza logaritmica negativa. Questi punti (se individuati) avrebbero costituito le anomalie.

Innanzitutto, si normalizzano tutte le caratteristiche al fine di avere valori compresi tra zero e uno e rendere questi ultimi adatti allo stimatore basato sul gradiente. La lunghezza della previsione, ovvero l'orizzonte di previsione, sarà composta da 24 ore moltiplicate per i giorni da prevedere.

È stato tracciato l'intervallo di previsione al 90%, l'intervallo di previsione al 50% e la previsione mediana. Questi valori sarebbero stati confrontati con i valori osservati nei dati di *test* al fine di individuare comportamenti sospetti legati all'uso delle applicazioni bancarie.

Come si vede nella figura 5, l'attività normale dell'utente alla data presa in considerazione, rientra nell'intervallo di previsione ed è un indicatore dell'assenza di anomalie.

Nella figura 6 si può chiaramente osservare un comportamento anomalo. Per valutare meglio l'anomalia, è necessario estendere il periodo come nella figura 7 per vedere che la previsione effettuata dal modello e basata sulla serie temporale considerata è completamente diversa da quanto sta accadendo.

Introduciamo la figura 8, dove la linea rossa indica il comportamento osservato e individuato dal modello su scala più ampia (basata sulla massima verosimiglianza logaritmica negativa), solo per mostrare chiaramente come il modello esamini il comportamento su diverse dimensioni e non effettui un'analisi "ingenua" *sic et simpliciter* su picchi unidimensionali.

Infine, esaminiamo la valutazione del modello. Otteniamo un MSE (Errore quadratico medio) di 0,02, un MASE (Errore assoluto medio) di 1,13 e un rMSE (Errore quadratico medio normalizzato) di 0,15.

Questo ha portato alla rilevazione di operazioni sospette di frode sull'applicazione bancaria relativa agli assegni in filiale e, con lo stesso metodo, è stato possibile rilevare e bloccare un tentativo di esfiltrazione di dati sensibili.

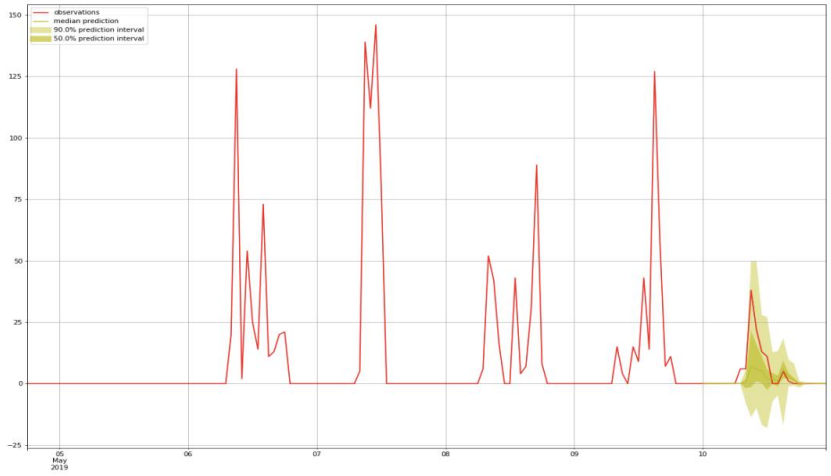


Figura 5: comportamento normale.

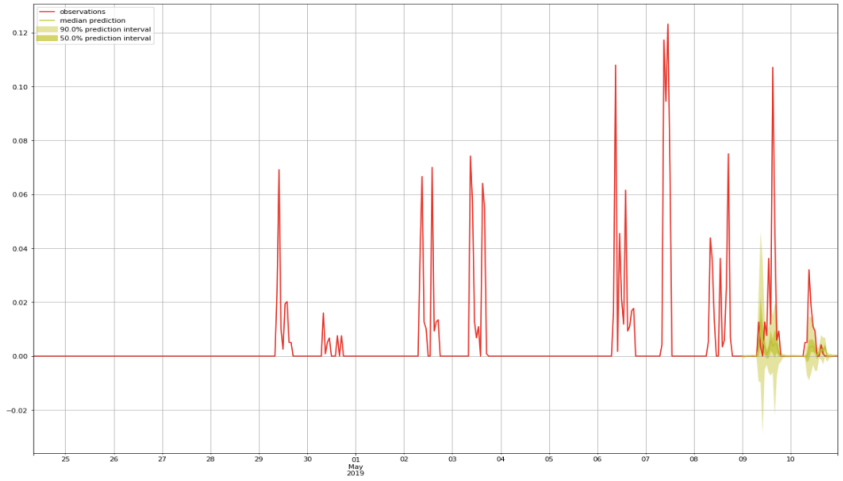


Figura 6: Comportamento anomalo con *forecast* di 2 giorni.

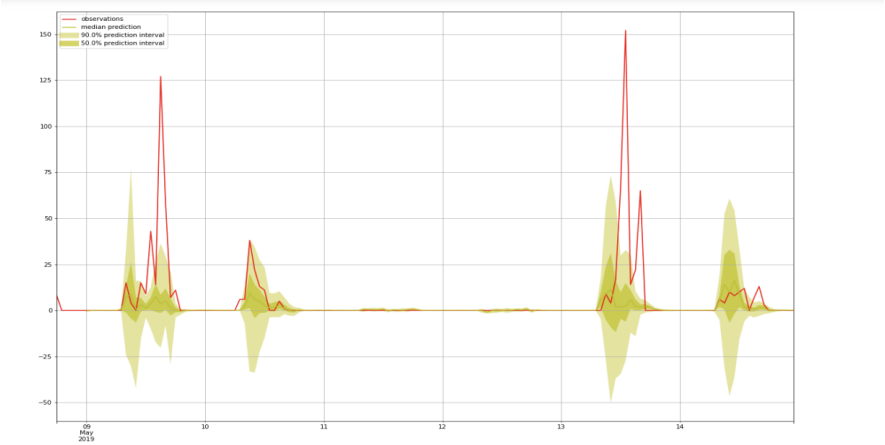


Figura 7: comportamento anomalo con un *forecast* di una settimana.

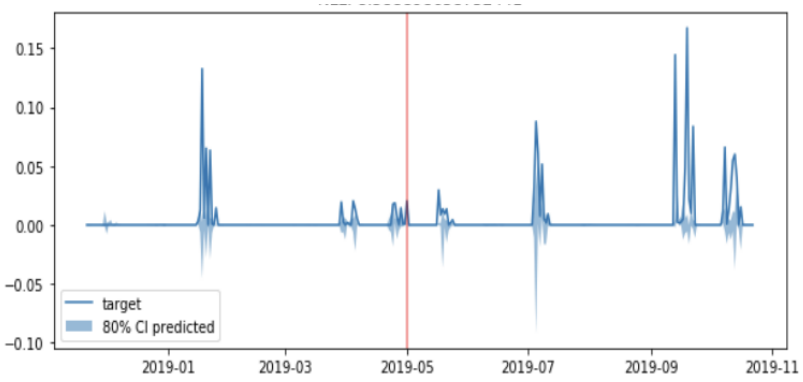


Figura 8: Anomalia (in rosso) per mostrare come i modelli di AI non guardino solo al "picco" ma al comportamento generale.

- Caso 2[253].

I sistemi di Antiriciclaggio (AML) vengono implementati dalle istituzioni finanziarie come le banche e altre istituzioni che forniscono credito, con

[253] J. HAN – Y. HUANG – S. LIU ET AL. *Artificial intelligence for anti-money laundering: a review and extension.* Digit Finance 2, 211–239 (2020).

l'obiettivo di contrastare il riciclaggio di denaro, identificando rischi, potenziali riciclatori e transazioni illecite. Il modo in cui le istituzioni finanziarie gestiscono la loro attività, i rischi che assumono e le politiche che implementano (o non implementano) devono superare l'esame di terze parti, tra cui clienti, azionisti, governi e regolatori. Non raggiungere gli standard AML richiesti è una forma di scorrettezza aziendale, che comporta anche un forte rischio reputazionale.

Il Gruppo Wolfsberg[254], formato da un insieme di banche internazionali per condividere idee sulla lotta al riciclaggio di denaro globale, si è riunito all'inizio del 2002 per discutere le conseguenze degli attacchi terroristici dell'11 settembre.

Ciò che preoccupava il comitato e le agenzie internazionali era il fatto che l'intera operazione terroristica avrebbe potuto essere finanziata con meno di 500.000 dollari; una somma esigua rispetto alle normali transazioni bancarie. Come potevano le banche, che gestivano centinaia di milioni di dollari al giorno, individuare attività sospette in transazioni di importi così ridotti come 2.000-5.000 dollari? Come avrebbero potuto individuare il finanziamento terroristico dietro gli eventi dell'11 settembre?

[254] Il Gruppo Wolfsberg è stato costituito nel 2000, nel castello di Wolfsberg, che si trova nella Svizzera nord-orientale. Rappresenta un organismo non governativo e indipendente, composto (fino ad oggi) da 13 banche, che operano nel settore dei servizi finanziari e dei prodotti correlati.

Due anni dopo, quasi la metà delle prime 20 banche mondiali utilizzavano sistemi di intelligenza artificiale che da quel momento costituiscono il principale metodo nella lotta al riciclaggio di denaro.

- Cenni teorici.

Il collocamento, la stratificazione e l'integrazione sono le tre fasi negli schemi di riciclaggio di denaro. I proventi delle attività criminali entrano nella fase di collocamento, dove vengono convertiti in strumenti monetari o depositati in un'istituzione finanziaria. La stratificazione si riferisce al trasferimento di fondi ad altre istituzioni finanziarie o ad individui tramite bonifici bancari, assegni, vaglia postali o altri metodi. Nella fase finale di integrazione, i fondi vengono utilizzati per acquistare beni legittimi o per continuare a finanziare imprese criminali. In questi casi, il denaro ottenuto illegalmente diventa parte dell'economia legittima.

Gli approcci basati sull'intelligenza artificiale possono essere impiegati per identificare le attività di riciclaggio di denaro nelle suddette tre fasi. Metodi tradizionali di apprendimento automatico, come le *Support Vector Machines* (SVM) e le *Random Forest* (RF), possono essere utilizzati per classificare transazioni fraudolente, facendo uso di ampi *dataset* bancari annotati. Questi approcci basati sui dati sono tipicamente adoperati nelle fasi di collocamento e stratificazione, in quanto i dati delle transazioni sono attenzionati da parte della banca. La fase finale di integrazione risulta invece, difficile da

individuare, in quanto i fondi hanno eluso i meccanismi di rilevamento delle frodi. In questa fase, metodi avanzati di intelligenza artificiale, come l'estrazione delle relazioni tra entità da ampi dati di *social media* e notizie, potrebbero essere applicati all'*Anti-Money Laundering* (AML). Una volta individuate le transazioni sospette mediante sistemi basati sull'apprendimento automatico, un investigatore specializzato nell'individuazione di attività fraudolente, si impegna in procedure analitiche successive. Il carico di lavoro dell'investigatore umano dipende principalmente dal numero di transazioni fraudolente segnalate. Approcci di elaborazione del linguaggio naturale (NLP) all'analisi delle entità e delle relazioni possono alleggerire il compito, fornendo agli esperti umani un punteggio e una rappresentazione visuale delle relazioni basati su dati di notizie (come, ad esempio, il *database* delle notizie delle banche e fonti di notizie tradizionali o social media) riguardo all'entità potenzialmente fraudolenta, sfruttando tecnologie basate su NLP.

Le istituzioni finanziarie stanno adottando tecnologie avanzate di analisi statistica e dati nei loro approcci di *Anti-Money Laundering* (AML) per ridurre i rischi e i costi dell'ispezione manuale. Questo livello di approccio si basa su decisioni storiche e confronti con transazioni simili per determinare se una transazione sospetta richiede una revisione manuale. Se una transazione viene segnalata, vengono aggiunti dati supplementari per la valutazione, tra cui cronologia delle decisioni simili, punteggi di rischio dai livelli precedenti e priorità di liquidazione.

L'analisi delle reti è un metodo per individuare attività di riciclaggio di denaro. In ambito di ricerca AML, l'analisi delle reti si riferisce agli studi che utilizzano dati relazionali per individuare connessioni dirette e nascoste con nodi di riciclaggio di denaro. Quest'ultima inizia con la valutazione della centralità, usata per determinare il nodo più importante in una rete. Le variabili comuni dell'analisi delle reti includono: grado di centralità, autorità, centralità di intermediazione, centralità di vicinanza, *hubness* e *page rank*. La centralità di grado misura le connessioni dirette di un nodo nella rete. L'autorità indica quanto un nodo punta ad un altro tramite *hub* importanti. Il *page rank* riflette l'importanza di un nodo sulla base del tempo trascorso su di esso rispetto agli altri nodi.

Il passaggio successivo è la creazione di un grafo tra entità. I collegamenti tra soggetti (rappresentati come nodi) derivano dalle transazioni che li mettono in collegamento. Queste idee si applicano anche al riciclaggio di denaro mobile. Creando grafi sintetici simili a reti sociali, si possono visualizzare e individuare connessioni specifiche. Questo metodo è stato testato su dati di documenti di testo riguardanti il riciclaggio di denaro. L'analisi dei collegamenti rappresenta le connessioni tra entità (soggetti, organizzazioni, conti bancari) e può essere potenziata con metodi di apprendimento automatico per migliorare i collegamenti e l'informazione catturata dal grafo. Un altro approccio naturale nell'uso dell'intelligenza artificiale e del *data mining* - per individuare riciclaggio e frodi - è la rilevazione di anomalie. Si stabilisce come dovrebbe apparire una transazione normale per un soggetto e

si identificano transazioni notevolmente diverse da queste per considerarle anomalie. Si crea un gruppo di riferimento per catturare le abitudini di spesa tipiche dei clienti, impiegando spesso il *clustering*. Successivamente, si calcola la distanza tra le transazioni in arrivo e il gruppo di riferimento per individuare comportamenti anomali. Esempi includono l'uso del *clustering k-means* per raggruppare i dati e rilevare anomalie tramite distanza dai *cluster* o la classificazione di transazioni in arrivo in base alla deviazione da *cluster*, usando dati di transazioni reali. Questi approcci rafforzano l'individuazione di potenziali attività fraudolente e di riciclaggio di denaro in ambito finanziario.

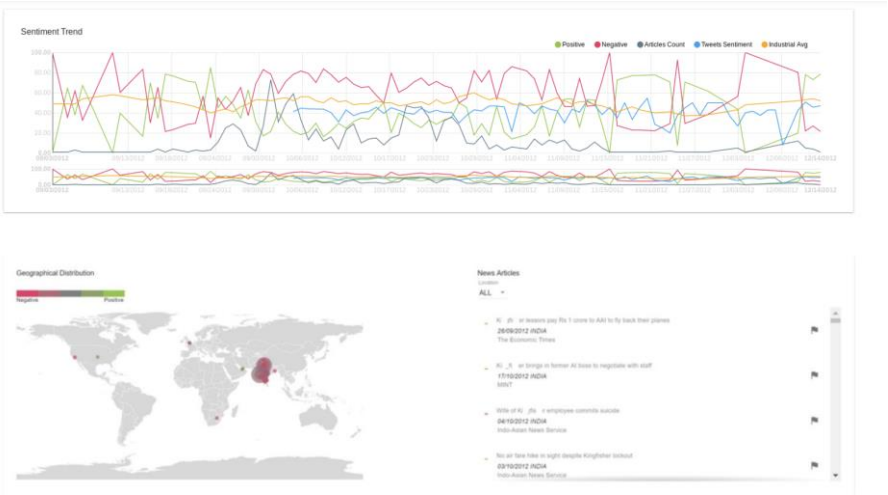
A differenza delle metodologie convenzionali di *machine learning*, il *deep learning* consente l'estrazione di rappresentazioni delle caratteristiche dai dati grezzi. Questo processo coinvolge lo sviluppo di strati multipli di rappresentazioni partendo da *input* non elaborati, attraverso manipolazioni non lineari a ciascun livello.

Un esempio è l'elaborazione del linguaggio naturale (NLP), sottocampo dell'AI che impiega tecniche per l'analisi sintattica, semantica e discorsiva, estrazione e classificazione del testo, traduzione automatica.

Nel campo della conformità AML, NLP e *deep learning* sono utilizzati a vari livelli.

- Uso dell'AI.

Quando gli investigatori AML individuano un'azienda potenzialmente coinvolta in una transazione sospetta, solitamente consultano *Internet* per reperire prove. Analizzare i livelli di *sentiment* delle notizie riguardanti una specifica organizzazione può rivelare una quantità significativa di prove; ad esempio, le tendenze costantemente negative e le parole chiave negative associate all'azienda *Kingfisher* (oggetto di esempio nel prosieguo del lavoro) possono aiutare gli investigatori umani a scoprire rapidamente le attività fraudolente o di riciclaggio di denaro dell'azienda. L'analisi del *sentiment* basata su AI e NLP può esaminare migliaia di articoli in pochi secondi, migliorando notevolmente il processo investigativo in termini di efficienza e precisione e può anche essere utilizzata nei processi di monitoraggio del profilo del cliente e di accoglienza del cliente, per esaminare e identificare punti critici specifici di un cliente e la sua associazione con articoli negativi.



Trend del *sentiment* dell'azienda Kingfisher Airlines.

La fonte dei dati per questo studio è stata un ampio *corpus* di notizie. È stato utilizzato un *Recurrent Neural Network* (RNN) per classificare gli articoli di notizie come positivi, negativi o neutri. Sono stati generati punteggi per ciascuna delle categorie, compresi tra "positivo" e "negativo". La figura descrive le tendenze complessive del *sentiment* presenti nelle notizie riguardanti *Kingfisher Airlines*. La linea grigia nel grafico indica il numero di articoli/notizie al giorno, e la linea rossa indica il punteggio aggregato per il *sentiment* negativo (al giorno). Le dimensioni dei cerchi sovrapposti alla mappa del mondo, rappresentano il numero di occorrenze del termine "Kingfisher Airlines" nelle notizie in quella regione, e il colore trasmette il *sentiment*. Il verde è positivo, il grigio è neutro e il rosso è negativo. Un *sentiment* negativo costantemente elevato verso l'organizzazione in un certo periodo potrebbe indicare un potenziale candidato per il blocco. Inoltre, l'applicazione dell'estrazione dei termini di aspetto durante questo periodo può rivelare le cause del *sentiment* negativo.

- Caso 3[255].

Le manipolazioni di titoli sono attività illegali in cui vengono realizzati comportamenti insoliti per ingannare i prezzi e i volumi nei mercati di

[255] S. SRIDHAR - S. MOOTHA, *Stock market manipulation detection using feature modelling with hybrid recurrent neural networks*, in *International Journal of Networking and Virtual Organisations*, Vol. 26, No. 1-2.

negoziazione. La manipolazione delle azioni crea scambi ingiusti, che possono causare enormi danni all'integrità dell'industria finanziaria. Gli studiosi Allen e Gale (1992) hanno classificato le manipolazioni di titoli in tre tipi di base: manipolazione basata sull'azione, manipolazione basata sull'informazione e manipolazione basata sul commercio. La manipolazione basata sull'azione coinvolge la modifica della domanda e dell'offerta di un'azienda; variabile che influenza il cambiamento di prezzo. La manipolazione basata sull'informazione riguarda la diffusione di false voci per ingannare il valore dell'azienda. La manipolazione basata sul commercio mira a manipolare i mercati eseguendo ordini di acquisto/vendita elaborati con alcune strategie per influenzare i prezzi delle azioni. Tra questi tipi, la manipolazione basata sul commercio ha attirato maggiormente l'attenzione delle ricerche sulla rilevazione delle manipolazioni di titoli, poiché tutti i comportamenti dei *trader* possono essere osservati attraverso il registro di *trading* del mercato. Tuttavia, riconoscere la presentazione di ordini manipolativi non è un compito facile a causa della grande quantità di dati generati dalle piattaforme di *trading* computerizzate ad alta velocità. Il comportamento manipolativo, che è una minoranza, verrà nascosto da queste attività di *trading* legittime. Inoltre, i manipolatori faranno del loro meglio per nascondere le loro intenzioni, rendendo ancora più difficile la rilevazione. L'uso dell'AI è efficace per la rilevazione della manipolazione dei titoli poiché può apprendere le caratteristiche chiave di vari modelli manipolativi, che sono stati sviluppati in modi diversi per evitare di essere notati.

- Cenni teorici.

Negli ultimi anni, la ricerca sulla rilevazione della manipolazione dei titoli è stata condotta sia in modo supervisionato che non supervisionato. Il primo metodo costruisce relazioni tra le caratteristiche di *input* e i modelli di manipolazione identificati; quindi, richiede la conoscenza dell'etichettatura precedente. Invece, l'apprendimento non supervisionato utilizza algoritmi di *clustering* o forma una distribuzione dei dati normali per distinguere gli *outlier* senza informazioni di etichettatura. Entrambe le modalità hanno vantaggi e svantaggi. Per l'apprendimento supervisionato, creare etichette per coprire vari modelli di manipolazione è laborioso e difficile. Un altro punto debole significativo dell'apprendimento supervisionato è che può riconoscere solo schemi di manipolazione noti che erano nel *database* di addestramento, ma non può riconoscere modelli di manipolazione non "visti" in precedenza. Come accennato, i manipolatori adattano regolarmente le loro tecniche per evitare di essere scoperti. Al contrario, l'apprendimento non supervisionato è utile per riconoscere modelli di manipolazione mai visti prima, ma generalmente con una precisione inferiore rispetto all'apprendimento supervisionato.

In un caso importante è stato utilizzato un modello di *autoencoder* non supervisionato per rilevare manipolazioni di titoli basate sul commercio nella

Borsa di Bangkok (SET) durante il periodo 2004-2016 e sono stati segnalati sei casi.

La rilevazione della manipolazione del mercato azionario coinvolge l'individuazione di caratteristiche nelle transazioni che indicano la presenza di frodi. Queste caratteristiche possono essere statiche o sequenziali.

Le caratteristiche singole che indicano la manipolazione in un particolare istante sono le caratteristiche statiche del *dataset.* Queste ultime non cambiano con la variazione nel tempo. Alcune delle caratteristiche statiche includono il volume totale alla fine della giornata, la quantità consegnabile di azioni, la percentuale della quantità consegnabile rispetto alla quantità di azioni scambiate, la differenza tra massimo e minimo e la differenza tra apertura e chiusura.

Le reti neurali artificiali basate su *perceptron* multistrato (MLP) modellano le caratteristiche statiche del *dataset*. Queste includono il volume e il prezzo delle azioni in un determinato momento, il volume totale, la quantità consegnabile, la differenza tra massimo e minimo e tra apertura e chiusura. Queste caratteristiche sono specifiche in un particolare istante.

Le reti neurali sono usate insieme per aumentare la precisione nella rilevazione delle manipolazioni utilizzando caratteristiche statiche. I modelli di *ensemble* (combinazione di diversi algoritmi) imparano come combinare le uscite dei sotto-modelli per ottenere una migliore precisione e una ridotta perdita.

Le caratteristiche sequenziali dipendono dal tempo. Queste sono caratteristiche varianti nel tempo che aiutano a identificare le tendenze nel *dataset*. Alcune delle caratteristiche dinamiche sequenziali sono il cambiamento nei prezzi di apertura, massimi, minimi, chiusura (OHLC) e le medie mobili semplici (SMA) di questi prezzi. Le caratteristiche dinamiche aiutano a rilevare la manipolazione che avviene nel corso del tempo.

Le reti neurali ricorrenti (RNN) modellano i dati varianti nel tempo ed estraggono schemi che si verificano negli *input*. La manipolazione del mercato azionario avviene nel tempo. Questi aspetti temporali dei dati sono modellati utilizzando RNN nella forma di memoria a lungo termine (LSTM) e memoria a lungo termine bidirezionale (Bi-LSTM). Le LSTM aiutano a determinare la variazione dei prezzi e dei volumi delle azioni in relazione alle transazioni precedenti nel corso del tempo. Aiutano a identificare la dipendenza temporale all'interno del *dataset* ricordando i dati passati e costruendo un modello tra i dati attuali e quelli passati. Le Bi-LSTM aiutano il sistema a prevedere la possibile verificazione di una manipolazione in futuro. Questo avviene apprendendo le caratteristiche dei dati in entrambe le direzioni.

- Uso dell'AI.

I manipolatori potrebbero cercare di mascherare le caratteristiche dell'operazione affinché le transazioni non vengano segnalate dai sistemi di

rilevamento. Al fine di modellare in modo efficace sia gli aspetti statici che temporali dei dati, è stato implementato un sistema ibrido di ANN basato su MLP e reti neurali ricorrenti. Vengono utilizzate sia le RNN basate su LSTM che su Bi-LSTM. Ciò aiuta a chiarire l'impatto dei dati varianti nel tempo insieme ai dati statici nella determinazione delle manipolazioni di mercato.

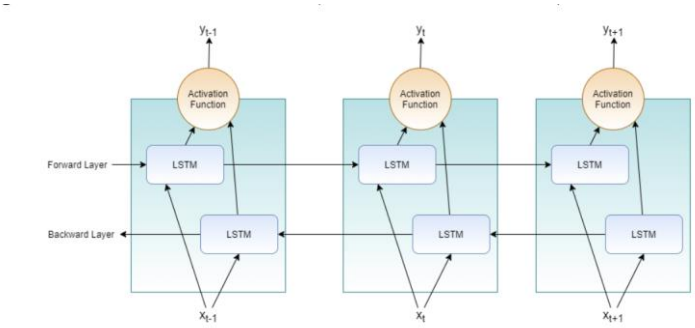
Il *dataset* utilizzato contiene un totale di 20 attributi, che possono essere categorizzati come statici o dinamici. Le caratteristiche statiche sono quelle che cambiano in tempo reale. In termini di mercato azionario, queste includono i dati OHLC (apertura, massimo, minimo e chiusura) a fine giornata, il prezzo medio ponderato (WAP), il numero di azioni, il numero di scambi, la quantità consegnabile, il volume totale, la percentuale di quantità consegnabile rispetto alla quantità scambiata, lo *spread* tra massimo e minimo e lo *spread* tra apertura e chiusura. Questi sono valori unici e variano ogni giorno e non dipendono da quelli pregressi. Le caratteristiche dinamiche sono quelle che dipendono dal tempo e possono essere calcolate solo se i valori precedenti sono noti. Queste caratteristiche includono la variazione nei prezzi OHLC tra i giorni e la SMA (media mobile semplice) dei prezzi OHLC nel periodo di analisi. Queste caratteristiche aiutano a identificare le tendenze nel mercato azionario. Ogni campione nel *dataset* iniziale è stato etichettato come 0 se quel campione non è stato manipolato, altrimenti come 1. Tutti i valori sono stati puliti, elaborati e normalizzati.

Il modello ANN-RNN modella contemporaneamente le caratteristiche statiche e dinamiche del *dataset*. Questo aiuta il modello ibrido a

comprendere la variazione dei prezzi e dei volumi che potrebbero essere un'indicazione dell'occorrenza di manipolazione. Gli algoritmi di apprendimento automatico e le reti neurali *feedforward* possono gestire solo *dataset* statici. Non possono modellare le variazioni nei dati che si verificano dinamicamente. Utilizzando un modello ibrido, si combinano gli aspetti temporali dei dati sequenziali con gli aspetti spaziali dei dati statici. Il modello ibrido ottiene le migliori prestazioni su sequenze di lunghezza ridotta, con accuratezze del 96,06% e del 92,02%, rispettivamente. Il modello ibrido ANN-LSTM performa meglio del modello ibrido ANN-BiLSTM. Questo perché tratta dati finanziari che dipendono solo dal passato e non dal futuro. Il modello non può determinare efficacemente se si verifichi o meno una manipolazione quando legge dati futuri, poiché la manipolazione può essere identificata solo attraverso variazioni storiche dei prezzi/volumi e non mediante variazioni future. Il modello di insieme, nonostante una precisione del 96%, utilizza cinque sotto-modelli; ciò aumenta la complessità di addestramento. Quest'ultimo apprende solo le caratteristiche statiche e quindi può rilevare la manipolazione solo in un istante specifico. Non tiene conto della variazione dei parametri nel tempo e quindi non modella le fluttuazioni nel *set* di caratteristiche varianti nel tempo. I dati dinamici modellati separatamente con LSTMs e BiLSTMs hanno un'accuratezza molto elevata del 99% nel rilevare le manipolazioni, ma questo non tiene conto delle caratteristiche statiche e quindi sovra-adatta quelle per il rilevamento della manipolazione. Le variazioni nei prezzi dovrebbero essere correlate a

caratteristiche statiche come il volume degli scambi di azioni, determinando un apprendimento più generico dei dati. Le caratteristiche dinamiche richiedono grandi sequenze di scenari di manipolazione possibili al fine di ottenere un modello che non sia né sotto-adattato né sovra-adattato. Quest'ultimo può quindi essere esteso a qualsiasi *dataset* che tratta manipolazioni di mercato. La combinazione degli aspetti spaziali e temporali dei dati porta a una modellazione accurata della varianza del *dataset* e quindi alla creazione di un modello in grado di gestire cambiamenti periodici dei dati.

I classificatori raggiungono una previsione di veri positivi al 100% avendo falsi positivi trascurabili.



Struttura di un modello Bi-LSTM.

- Caso 4.

Il problema dell'esfiltrazione illecita dei dati si è spesso presentato all'attenzione della Suprema Corte che ha sviluppato un importante dibattito sul tema.

Si pensi al caso di un soggetto che al fine di svolgere attività professionale privata si introduca nel sistema informatico dello studio per il quale lavori ed effettui il *backup* dei dati in esso inseriti.

In concreto, si tratta di un soggetto che ha l'autorizzazione ad accedere al sistema, ma la utilizza per eseguire un'attività non consentita dal titolare del sistema.

Il nodo fondamentale riguarda la configurazione del reato di accesso abusivo a sistema informatico di cui all'art. 615-ter c.p.[256]

[256] Per un approfondimento sulla fattispecie di accesso abusivo a sistema informatico di cui all'art. 615-ter c.p. si veda: L. PICOTTI, *Studi di diritto penale dell'informatica*, Verona, 1992; L. PICOTTI, voce, *Reati informatici*, in *Enc. Giur.*, *Agg*., VIII, Roma, 2000, 1 ss; F. BARGHELLA - R. BLAIOTTA, *Diritto penale dell'informatica e beni giuridici*, in *Cass. Pen.*, 1995, 9, 2329 ss. Per un riferimento alla Convenzione del Consiglio d'Europa del 2001 sul Cybercrime ed alla legge di ratifica n. 48 del 2008, tra gli altri, L. PICOTTI, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir. Pen. Proc.*, 2008, 700 ss P. GALDIERI, *Teoria e pratica dell'interpretazione del reato informatico*, Milano 1997, 147; R. BORRUSO, *La tutela del documento e dei dati*, in R. BORRUSO - D. BUONOMO - G. CORASANITI - G. D'AIETTI, *Profili penali dell'informatica*, Milano 1994, 28; D. PLANTAMURA, *Moderne tecnologie, riservatezza e sistema penale: quali equilibri?*, in *Dir. inf. e informatica*, 2006, 417 ss.; R. FLOR, *Verso una rivalutazione dell'art. 615-ter c.p.?*, in *Dir. pen. cont.*, 2012, 2, 131; M. BELLACOSA, *Il luogo di consumazione del delitto di accesso abusivo a un sistema informatico o telematico: in attesa delle Sezioni unite*, in *Dir. pen. cont.*, 2 febbraio 2015, 6; F. FASANI, *Accesso abusivo a un sistema informatico: le Sezioni unite cambiano di nuovo rotta*, in *Riv. Società*, 2017, 1404; G. FIANDACA - E. MUSCO, *Diritto penale, parte speciale*, Bologna - Roma 2013, II t. I, 293; F. MANTOVANI, *Diritto penale pt. sp.*, Padova, 2016, I, 577; C. PECORELLA, *Diritto penale dell'informatica*, Padova, 2006, p. 322 ss.; ID, *L'attesa pronuncia*, cit., 3692 ss; C. PIERGALLINI, *I delitti contro la riservatezza informatica*, in C. PIERGALLINI - F. VIGANO' - M. VIZZARDI - A. VERRI, in *Trattato di diritto penale, pt. sp.*, diretto da G. MARINUCCI - E. DOLCINI, Milano, 2015, X, 772 ss.; Vedi anche I. SALVADORI, *L'accesso abusivo ad un sistema informatico o telematico. Una fattispecie*

- L'analisi giurisprudenziale.

La Corte di Cassazione chiamata a pronunciarsi sulla questione[257], ha affermato che "decisiva, quindi, per giudicare la liceità dell'accesso effettuato da chi sia abilitato ad entrare in un sistema informatico, è per la giurisprudenza di legittimità la finalità perseguita dall'agente che deve essere confacente con la *ratio* sottesa al potere di accesso, il quale mai può essere esercitato in contrasto con gli scopi che sono alla base dell'attribuzione del potere, nonché in contrasto con le regole dettate dal titolare o dall'amministratore del sistema".

Nel caso in oggetto l'agente era in possesso di un titolo valido di legittimazione, quindi, è da escludere l'abusività dell'acceso ai sensi del primo comma dell'art. 615-ter c.p., si deve quindi considerare se il mantenimento nel sistema fosse da qualificare in contrasto con la volontà del titolare dello stesso.

La Suprema Corte in questo caso valuta la condotta da un punto di vista soggettivo, soffermandosi sulle finalità ulteriori che spingono il soggetto ad accedere al sistema informatico; una tale interpretazione, secondo parte della

paradigmatica dei nuovi beni giuridici emergenti nel diritto penale dell'informatica, in Tutela penale della persona e nuove tecnologie, Padova, 2013, 147.

[257] Cass. Pen., Sez. V, 2.10.2020, n. 34269.

dottrina si pone in contrasto con il dato letterale della norma e sembra essere mossa dall'esigenza di criminalizzare la condotta.

In casi come questo la domanda che ci si dovrebbe porre è: sussiste un divieto oggettivo espresso o tacito all'accesso al sistema per effettuare il *backup* dei dati in esso contenuti?

Infatti, oggetto di indagine non deve essere la condotta successiva rispetto all'accesso o al mantenimento nel sistema, in quanto, l'abusività - stando al dato letterale della norma - deve essere riferita all'accesso e non alla condotta eventualmente illecita posta in essere in un momento temporalmente diverso[258].

Le prospettive di riforma dell'accesso abusivo di cui all'art. 615-ter c.p. alla luce delle nuove tecnologie.

[258] L'art. 615-ter c.p. è speculare rispetto all'art. 614 c.p. che incrimina la violazione di domicilio.
Mettendo da parte per un attimo l'accesso abusivo a sistema informatico, si prenda ad esempio la condotta di un soggetto autorizzato ad accedere nell'abitazione di un altro soggetto, che però vi faccia ingresso per compiere un furto. Nel caso in esame quale sarebbe il reato contestato? Sicuramente il furto, in quanto l'accesso era autorizzato e oltretutto il reato di violazione di domicilio si consuma con l'introduzione nell'abitazione, pertanto, non si guarda alla condotta ulteriore posta in essere. La configurabilità della violazione di domicilio si basa sullo *ius excludendi* del titolare (per quanto attiene l'accesso) e sulle regole impartite dallo stesso (in relazione alla permanenza). Il domicilio informatico tutelato da misure di sicurezza si intende violato quando vi si acceda o vi si permanga in assenza di legittimazione oggettiva, desumibile dagli obblighi imposti dal titolare dello stesso.

L'analisi giurisprudenziale sembra dimostrare che l'interpretazione spesso travalica il dato letterale della norma e sembra essere mossa dall'esigenza di criminalizzare comportamenti che – sebbene in astratto siano illeciti – non rispondono alla fattispecie delineata in origine dal legislatore.

Le nuove tecnologie – come si è visto – possono avere un duplice ruolo: possono incrementare condotte illecite mediante l'utilizzo di algoritmi che nella maggior parte dei casi sono sconosciuti per gli investigatori, ma possono avere anche un ruolo centrale nell'attività investigativa al fine di individuare gli autori delle condotte illecite poste in essere in rete o su supporti elettronici.

Nel caso esaminato, l'utilizzo di tecnologie avanzate potrebbe aiutare ad individuare le condotte che si pongono in contrasto con lo schema autorizzativo fornito dal titolare del sistema; si pensi ad esempio, alla procedura delineata nel "Caso 1"[259]; quest'ultima consentirebbe una rilevazione dell'anomalia del *log* che non corrisponde alle caratteristiche individuate in fase di autorizzazione all'accesso o al mantenimento nel sistema.

Orbene, al termine di questa breve analisi casistica si può rilevare che solo coniugando le competenze tecniche con quelle giuridiche si potranno avere degli sviluppi nel settore della c.d. industria 4.0 che permettano di contemperare gli interessi in gioco e di sfruttare al massimo le potenzialità della tecnologia.

[259] Si veda *supra*: Caso 1.

CAPITOLO IV

Verso una regolamentazione europea dei sistemi di intelligenza artificiale. Problemi e prospettive.

1. Il quadro normativo di riferimento a livello europeo in tema di digitalizzazione. - 1.1 Il *Digital Service Act*. - 1.2 Linee guida etiche in materia tecnologica. - 2. L'AI Act. Una proposta di Regolamento. - 2.1 La definizione degli attori e l'approccio basato sul rischio. - 3. Le differenze con l'approccio di *soft law* americano. - 4. La sostenibilità di una *compliance* automatizzata alla luce del quadro normativo europeo.

1. Il quadro normativo di riferimento a livello europeo in tema di digitalizzazione.

L'innovazione tecnologica rende necessario lo sviluppo di nuove infrastrutture che consentano di gestire attività sia pubbliche che private nel minor tempo possibile mirando ad una sostanziale riduzione dei costi.

Quando si parla di digitalizzazione e di nuove tecnologie non si può tralasciare un tema centrale rappresentato dalla tutela dei diritti fondamentali dei soggetti coinvolti.

L'Unione Europea è intervenuta su vari fronti, tra i contributi più importanti, ai fini della presente ricerca si trovano: il Regolamento in materia di protezione dei dati personali, il *Digital Service Act* (DSA) ed il *Digital Market Act* (DMA) e da ultimo la proposta di Regolamento in materia di Intelligenza Artificiale.

La prospettiva europea attuale si basa sull'Agenda Digitale per il 2030, che fissa gli obiettivi strategici da attuare nel decennio in corso.

Il programma prevede una cooperazione annuale per conseguire obiettivi e traguardi comuni.

La digitalizzazione e più nello specifico l'utilizzo di sistemi di intelligenza artificiale richiedono però, un bilanciamento tra due opposte esigenze: da un lato, l'obiettivo è sviluppare strumenti tecnologici sempre più avanzati mantenendo in questo modo alta la competitività delle imprese e delle infrastrutture europee sul mercato globale e dall'altro, si mira a tutelare i diritti dei soggetti che operano sul mercato e nei nuovi spazi tecnologici.

La Commissione europea nel 2018 pubblica una prima comunicazione sull'Intelligenza Artificiale per l'Europa analizzando il fenomeno tecnologico in relazione agli obiettivi di integrazione economica e competitività internazionale.

In questo primo documento la Commissione pone al centro la regolamentazione dell'utilizzo della tecnologia al fine di garantire la sicurezza e i diritti dei soggetti coinvolti.

Il Piano coordinato in materia di intelligenza artificiale del 2018 inquadra l'IA in una dimensione europea proprio per rendere possibile l'ottimizzazione degli investimenti e la realizzazione di collaborazioni transnazionali per accrescere la competitività delle imprese europee a livello globale.

La cooperazione tra i vari Stati e tra le infrastrutture pubbliche e le imprese private non sarebbe possibile senza l'accessibilità ai dati. Questo è il primo

obiettivo che il Programma individua. Non può esserci interoperabilità senza un accesso ai dati adeguato e volto allo sviluppo sistemi automatizzati di gestione e di controllo.

Inoltre, la Commissione si prefigge di consolidare la fiducia negli strumenti tecnologici garantendo la prevedibilità, la verificabilità ed il rispetto dei principi etici e dei diritti umani.

Nel 2020 viene pubblicato il Libro Bianco sull'intelligenza artificiale ed il documento relativo alla Strategia europea per i dati, insieme ad una Relazione sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e responsabilità.

Il Libro Bianco delinea in maniera più definita gli obiettivi della regolamentazione in materia di IA mirando a sviluppare una tecnologia di eccellenza che sappia creare fiducia negli utenti pubblici e privati.

La difficoltà che si rinviene nello sviluppo di una regolamentazione riguarda spesso l'opacità del sistema e la non conoscibilità a priori del risultato a causa della capacità della macchina di autoapprendere, ma anche all'estrema mutevolezza e vulnerabilità dell'informatica.

L'inadeguatezza del quadro normativo europeo rappresentato: dal Regolamento generale in materia di dati personali, dalla legislazione in materia di non discriminazione e dalla normativa sulle pratiche commerciali scorrette e la sicurezza generale dei prodotti, spinge la Commissione a ripensare le regole già esistenti, ma anche a prospettare nuove norme relative

alla fase di addestramento delle macchine, di tenuta dei dati e dei registri, alla trasparenza ed alla conoscibilità degli algoritmi sottesi.

Questi sono gli obiettivi delineati dalla proposta di Regolamento del 2021 e dalla Comunicazione sulla promozione di un approccio europeo all'intelligenza artificiale.

Le misure previste dalla Comunicazione sono volte a: promuovere investimenti nell'infrastruttura computazionale che sembra essere necessaria: per lo sviluppo di strumenti di intelligenza artificiale, il consolidamento di *network* di ricerca in materia di IA, lo sviluppo di criteri strutturali di sostenibilità accessibilità, sicurezza ed affidabilità ed alla definizione di settori strategici in cui l'intelligenza artificiale ha maggiori possibilità di sviluppo.

1.1 Il *Digital Service Act.*

L'Unione europea ha introdotto un pacchetto di norme volte a regolamentare il diritto dei servizi digitali e dei mercati digitali al fine di creare uno spazio digitale più sicuro per gli utenti e volto a realizzare pari condizioni per le imprese che vi operano[260].

[260] Per un approfondimento, tra gli altri, si veda: G.M. RUOTOLO, *Le proposte europee di riforma della responsabilità dei fornitori di servizi su Internet*, in *Riv. Italiana Informatica e Diritto*, 1, 2022; S. FLAMINIO, *Lotta alle fake news: dallo stato dell'arte a una prospettiva di regolamentazione per il "vivere digitale" a margine del Digital Services Act*, in *Riv. Italiana Informatica e Diritto*, 2, 2022; A. CHIMENTI, *La diffusione delle tecnologie digitali e le conseguenze nei campi del sapere e dell'informazione alla luce del quadro normativo europeo: l'impatto del Digital Markets Act e del Digital Services Act nel decennio digitale*

Quando si parla di servizi digitali ci si riferisce principalmente ai siti *web*, ai servizi di infrastruttura e alle piattaforme *online*.

Ogni individuo ogni giorno utilizza una piattaforma digitale - ad esempio, per fare acquisti, trovare informazioni, ascoltare musica - ma in assenza di un adeguato controllo e di regolamentazione i rischi possono essere maggiori rispetto ai vantaggi.

Le questioni problematiche riguardano il commercio e lo scambio di beni, servizi e contenuti illegali *online*, la compromissione di servizi *online* da parte di algoritmi manipolativi per alimentare la disinformazione o per cagionare danni a terzi, in quanto ciò determina un forte impatto sui diritti fondamentali.

L'UE con l'introduzione di questo pacchetto di norme mira a limitare i poteri di piattaforme - dette *gatekeeper* - che spesso agiscono sul mercato digitale come governanti privati riducendo la scelta dei consumatori e realizzando delle condizioni ingiuste per le imprese che le utilizzano.

Il principio fondamentale è: 'ciò che è illecito offline deve esserlo anche online'; quindi vengono enumerate e regolamentate una serie di operazioni a rischio in modo da minimizzarne l'impatto dannoso.

Per quanto riguarda la *governance* il DSA ha previsto due nuove figure: il *Compliance officer* ed il *Digital Services Coordinator*.

---

dell'UE, in *Nomos*, 2, 2023; C. CAUFFMAN – C. GOANTA, *A New Order: The Digital Services Ant and Consumer Protection*, in *Cambdrige university Press*, 2021; P. LEERSSEN, *An end to shadow banning? Transparency rights in the Digital Services Act beetween content moderation and curation*, in *Computer Law & Security Review*, 2023.

Il primo costituisce una figura interna all'impresa ed ha il compito di monitorare l'osservanza del regolamento, garantendo imparzialità e trasparenza di giudizio.

La seconda invece è una nuova autorità nazionale indipendente che deve vigilare sull'applicazione del regolamento con l'obbligo di trasparenza, imparzialità e tempestività, producendo un *report* annuale delle proprie attività.

Il *Digital Services Coordinator* ha il compito di garantire il coordinamento a livello nazionale sulle norme, di gestire i reclami contro i *provider* e di indagare sulla presenza di illeciti con potere di ispezione. L'Autorità può imporre la cessazione della violazione e la restrizione temporanea all'accesso al servizio interessato.

Il DSA è stato pubblicato in Gazzetta ufficiale Europea il 27 ottobre 2022 e troverà applicazione integrale entro il 17 febbraio 2024, salvo alcuni aspetti entrati in vigore già da novembre 2022.

1.2 Linee guida etiche in materia tecnologica.

La Commissione europea ha nominato un Gruppo[261] di esperti sull'intelligenza artificiale che ha elaborato delle linee guida al fine di

[261] Il Gruppo ha elaborato e pubblicato gli Orientamenti etici per un'IA affidabile ad Aprile 2019, al termine delle consultazioni con soggetti esperti e con i rappresentanti dei governi degli stati membri.

garantire affidabilità al sistema basandosi su tre componenti: una giuridica, una etica ed una inerente alla robustezza tecnica.

Le linee guida si prefiggono il rispetto dei diritti sanciti dai Trattati UE, dalla Carta dei diritti fondamentali e dal diritto internazionale in materia di diritti umani.

Alla base dei requisiti tecnici ed etici individuati si pongono i diritti fondamentali quali ad esempio: il rispetto della dignità umana, la libertà individuale, il diritto all'uguaglianza, alla non discriminazione e alla solidarietà.

Inoltre, i diritti civili sono posti a fondamento dei requisiti tecnici ed etici presi in considerazione; tra gli altri si fa riferimento al rispetto dell'autonomia umana, della *fairness*, del controllo umano, dell'*explicability*, della riservatezza e della *governance* dei dati, della diversità, equità, non discriminazione.

Il rispetto dell'autonomia umana richiede che le nuove forme di intelligenza artificiale non si sostituiscano all'uomo, ma lo assistano nelle proprie attività; in altre parole, secondo le linee guida l'utilizzo di sistemi di intelligenza "amplificata", anche se non vietato, dovrebbe essere considerato con cautela, perché potrebbe compromettere l'apporto decisionale umano.

Inoltre, l'intelligenza artificiale dovrebbe essere esente da discriminazioni e da distorsioni inique, a tal fine è necessario sviluppare un giusto contemperamento tra gli interessi in gioco e gli obiettivi prefissati.

L'algoritmo utilizzato deve essere spiegabile, nel senso che deve essere possibile comprendere il perché sia stata adottata quella decisione da parte della macchina, per fare ciò è necessario garantire la trasparenza rispetto alle capacità ed alle finalità degli strumenti adottati.

Quando le linee guida fanno riferimento alla robustezza intendono sottolineare che i sistemi devono essere capaci di far fronte agli eventuali errori commessi dall'algoritmo.

A tal fine, la sicurezza deve essere garantita dal momento della progettazione in modo da evitare il più possibile lo sviluppo di movimenti o di operazioni non verificabili.

Un altro elemento fondamentale è quello del controllo umano che può assumere in concreto varie accezioni: si potrebbe richiedere un intervento umano in ogni fase decisionale del sistema (*human-in-the-loop*); la supervisione potrebbe essere prevista nella fase di progettazione e di monitoraggio del sistema (*human-on-the-loop*); infine, il controllo umano potrebbe essere volto a controllare il complessivo funzionamento del sistema per decidere che operazione compiere in un dato momento (*human-in-control*).

Le linee guida mirano a garantire la riservatezza e la *governance* dei dati suggerendo un'implementazione della documentazione di ogni processo legato alla loro gestione.

Da questa analisi si può desumere che se da un lato il requisito tecnico richiede la tracciabilità delle operazioni realizzate dall'intelligenza artificiale dall'altro quello etico postula la conformità a specifici valori.

Gli Orientamenti etici[262] pongono al centro la decisione umana o meglio umanizzata che potrebbe avere l'effetto di limitare lo sviluppo della tecnologia in Europa rappresentando uno svantaggio in termini di competitività.

Si deve considerare che le linee guida non si esprimono riguardo ai valori che devono guidare il controllo umano sulle azioni dell'intelligenza artificiale, pertanto, si auspica un intervento chiarificatore in modo da rendere più agevole lo sviluppo e l'utilizzo delle macchine intelligenti.

2. *L'AI Act*. Una proposta di Regolamento.

L'intelligenza artificiale - come si è visto - è in rapida diffusione e rappresenta un fenomeno che non può essere arrestato o ignorato, ma che necessita di essere regolamentato. A tal proposito, la Commissione ha presentato una proposta di Regolamento dell'IA; come sottolineato nel *memorandum* di accompagnamento "l'obiettivo principale della proposta è garantire il corretto funzionamento della proposta è garantire il corretto funzionamento del mercato interno stabilendo norme armonizzate, in particolare sullo sviluppo,

[262] Per consultare il documento si veda: *https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai*.

l'immissione sul mercato dell'Unione e l'uso di prodotti e servizi che utilizzano le tecnologie di IA o forniti come IA autonoma di sistemi".

La Proposta rappresenta il primo quadro giuridico europeo sull'IA, fondandosi sui valori del *Bill of Rights* si propone di bilanciare i benefici ed i rischi per la salute dei consumatori e per i diritti fondamentali.

Alla base viene posta una valutazione dei rischi seguendo specifici indici di misurazione.

La Commissione attraverso il c.d. "Pacchetto IA" mira a realizzare un unico quadro giuridico (ritenuto dai più ingovernabile) adottando un approccio opposto rispetto a quello statunitense e cinese.

La scelta del Regolamento si pone in linea con l'obiettivo di fondo di non frammentare la regolazione, riducendo lo spazio di "manovra" da parte degli Stati.

Viene prospettato l'utilizzo della tecnica della "marcatura" già ampiamente utilizzata nel settore commerciale che prevede un controllo da parte dei privati a monte e lascia all'autorità pubblica solo un controllo a campione.

La marcatura CE garantisce la conformità ai requisiti richiesti dall'Unione; si pensi al caso di un sistema di intelligenza artificiale classificato "ad alto rischio" il quale per essere utilizzato, dovrà rispettare i requisiti previsti e quindi, si dovrà verificare che il sistema sia classificato ad alto rischio in base alle disposizioni regolamentari; attestare che la progettazione, lo sviluppo e il sistema qualitativo siano conformi alla normativa; introdurre una procedura di valutazione interna che autocertifichi la conformità; apporre una

dichiarazione di conformità ed infine, procedere con l'immissione del *software* sul mercato.

La marcatura CE non attesta la qualità oppure l'origine del prodotto, ma esclusivamente la conformità ai canoni previsti dall'Unione, volti alla tutela di interessi pubblici come la salute e la sicurezza degli utilizzatori del prodotto.

L'articolo 3, n. 1 definisce i sistemi cui si applica il Regolamento e fa riferimento a qualsiasi "*software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono*".

Orbene, da questa prima definizione si può rilevare che nella nozione di intelligenza artificiale non sono compresi solo i sistemi basati sull'apprendimento automatico, ma anche gli approcci basati sulla logica, sulla conoscenza e quelli statistici.

Un altro aspetto fondamentale riguarda l'individuazione dei soggetti che interagiscono nell'ambito del settore dell'IA che sono: il fornitore, l'utente, l'importatore ed il distributore[263].

[263] Il riferimento è a soggetti sia pubblici che privati i cui ruoli sono descritti nell'art. 3:
- Il fornitore può essere una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che sviluppa o fa sviluppare un sistema di intelligenza artificiale al fine di metterlo sul mercato o metterlo in servizio con il proprio nome o marchio, se a pagamento o gratuitamente.

La proposta di regolamento assume un perimetro di applicazione che va oltre i confini europei, in quanto prende in considerazione il prodotto messo in circolazione sul mercato europeo prescindendo dal luogo di produzione ed includendo tutti gli *output* utilizzati sul territorio dell'Unione.

Orbene, ciò comporta che qualunque prodotto sviluppato in un paese extraeuropeo potrà essere utilizzato nel territorio UE solo se conforme alle regole individuate dal Regolamento[264].

L'UE ha adottato un approccio basato sul rischio ed ha stabilito un diverso trattamento giuridico a seconda del rischio che si ipotizza per i diritti fondamentali dei soggetti coinvolti[265].

Particolare attenzione viene posta ai sistemi ad alto rischio, cui è dedicata la maggior parte della disciplina. Questi ultimi richiedono una particolare accuratezza nella gestione dei dati, la massima trasparenza rispetto al funzionamento della macchina e la possibilità del controllo umano.

- L'utente è qualsiasi persona fisica o giuridica, autorità pubblica o agenzia o altro organismo che utilizza un sistema di IA sotto la sua autorità, tranne nel caso in cui il sistema sia utilizzato nell'ambito di un'attività personale e non professionale.
- L'importatore può essere qualsiasi persona fisica o giuridica stabilita nell'Unione che immette sul mercato o mette in servizio un sistema di IA recante il nome o il marchio di una persona fisica o giuridica stabilita al di fuori dell'Unione.
- Il distributore è qualsiasi persona fisica o giuridica nella catena di approvvigionamento diversa dal fornitore o dall'importatore che mette a disposizione un sistema di IA sul mercato dell'Unione senza pregiudicarne le qualità.

[264] A. BRADFORD, *The Brussels Effect. How the European Union rules the world*, Oxford, 2020.

[265] L'*IA Act* individua varie categorie di rischio: in primo luogo vi sono sistemi vietati a causa dei rischi – considerati inaccettabili – che possono creare (art. 5); poi si individuano i sistemi ad alto rischio (art. 6); infine, vi sono i sistemi a rischio basso o minimo che possono circolare liberamente sul mercato, fermo restando alcuni obblighi di informazione, stabiliti a garanzia dell'utilizzatore (art 52).

Infine, la proposta di regolamento si sofferma sul sistema di verifica del rispetto dei requisiti individuati dalla disciplina riferita all'IA.

Il nodo centrale è proprio la garanzia di efficacia delle regole di funzionamento dei sistemi di IA. Nella maggior parte dei casi è il *provider* ad eseguire la verifica di conformità che consente la messa in commercio e l'utilizzazione del prodotto.

La decisione di adottare la tecnica dell'autocontrollo probabilmente rispecchia l'intento della Commissione di non limitare il progresso dell'IA prevedendo però – in caso di mancato rispetto della normativa – sanzioni severe[266].

Quindi, si può dire che l'Unione Europea abbia adottato un approccio volto da un lato a favorire lo sviluppo della tecnologia e dall'altro promuovere una regolamentazione organica ed uniforme in tutti gli Stati membri.

Il 14 giugno 2023 rappresenta per l'Europa una data "storica" in quanto è stata approvata dal Parlamento europeo la proposta di regolamento sull'intelligenza artificiale dando vita ad una delle regolamentazioni più avanzate in materia nel panorama mondiale.

3. Le differenze con l'approccio di *soft law* americano.

[266] A tal proposito, la proposta di regolamento all'art. 43 rinvia all'allegato III per determinare il tipo di procedura da seguire per il controllo di conformità (interna oppure esterna con l'intervento di un soggetto terzo); in questo modo la modifica dell'allegato consente di determinare la tipologia di controllo imposto al *provider*.

La regolazione dell'intelligenza artificiale è sentita come necessaria da parte delle grandi potenze mondiali in quanto, l'innovazione offre plurime opportunità, ma comporta dei rischi, determinati soprattutto dall'assenza di una normativa per la tutela gli interessi in gioco.

Gli Stati Uniti a differenza dell'Europa stanno adottando un atteggiamento meno restrittivo nei confronti dell'utilizzo della tecnologia.

Tuttavia, è stato osservato[267] da parte della dottrina, che già la definizione di intelligenza artificiale non è condivisa nel sistema americano; infatti, l'IA viene considerata al pari dell'intelligenza umana come una somma di abilità, sebbene abbia varie accezioni.

Però, la difficoltà regolatoria deriva anche dai rischi insiti nell'IA; in primo luogo, si tratta di strumenti nella maggior parte dei casi capaci di autoapprendere che rendono difficile il controllo sia da parte del programmatore che da parte dell'utilizzatore; in secondo luogo, trattandosi di sistemi in rapida evoluzione è necessario un costante aggiornamento anche della regolazione; infine, si deve tener conto della posizione degli Stati Uniti rispetto alle altre potenze mondiali – soprattutto riguardo alla Cina – in questo caso la differenza di approccio potrebbe rappresentare una penalizzazione qualora l'atteggiamento adottato si dimostri eccessivamente precauzionale.

[267] N. PETIT, *Law and Regulation of AI and Robots: Conceptual Framework and Normative Implications, working paper,* in *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2931339*; S.J. RUSSELL-P. NORVIG, *Artificial Intelligence, A Modern Approach*, 3 ed., *Edinburgh Gate*, Pearson, 2016.

L'attività regolatoria in materia di intelligenza artificiale ha preso il via con l'*Executive Order* 13859 dell'11 febbraio 2019 (*Maintaining American Leadership in Artificial Intelligence*). L'*Executive Order* 13859 individua quattro obiettivi principali che si riassumono: nella promozione della ricerca e dello sviluppo dell'intelligenza artificiale; la protezione della fiducia della popolazione nelle potenzialità della tecnologia; la formazione della forza lavoro capace di utilizzare l'IA; ed infine, la tutela delle scoperte degli Stati Uniti in materia di intelligenza artificiale.

Gli strumenti utilizzati sono di due tipi: finanziari e regolatori. I primi hanno lo scopo di promuovere l'intelligenza artificiale mentre i secondi si sviluppano su più fronti. La normazione si basa sia su interventi *ex post* – quindi essenzialmente di carattere casistico – che su disposizioni emanate *ex ante* che a loro volta sono sia di tipo pubblico (di competenza del Congresso e del potere esecutivo) sia di *self-regulation* (con il coinvolgimento dei giganti dell'industria *tech*).

La regolazione pubblica si estrinseca principalmente, nelle proposte legislative elaborate dal Congresso. Quest'ultimo ha dimostrato di promuovere lo sviluppo dell'intelligenza artificiale puntando a realizzare delle proposte che non pregiudichino l'innovazione.

Le iniziative adottate possono essere raggruppate in relazione allo scopo che intendono promuovere: in primo luogo, si possono riscontrare delle proposte volte a rafforzare la fiducia dei cittadini nell'impiego degli algoritmi. Si fa riferimento: all'*executive order* 13960 del dicembre 2020 (*Promoting the Use*

of Trustworthy Artificial Intelligence in the Federal Government), che stabilisce i principi generali in materia di IA[268]; *l'accountability framework* con il quale il *Government Accountability Office* ha declinato i principi da seguire nelle fasi di progettazione, sviluppo e monitoraggio dei sistemi di IA. Il *National Institute of Standards and Technology* ha elaborato e pubblicato un documento relativo all'individuazione dei *bias* nell'utilizzo dell'IA, operando una distinzione tra i vari tipi di *bias*; ad esempio, quelli concernenti i dati e quelli relativi all'impiego dell'IA.

Un secondo gruppo di atti in materia di intelligenza artificiale mira a promuoverne l'impiego da parte dell'amministrazione federale.

Il Congresso a dicembre 2020 ha approvato in via definitiva *l'Information Technology Modernization Centers of Excellence Program Act*, con il quale è stato avviato un ambizioso programma di transizione digitale con l'obiettivo di creare un centro di eccellenza sull'intelligenza artificiale nell'ambito della *General Services Administration* e di strutture simili appartenenti alle *executive agencies*.

[268] In base all'e.o. 13960 l'IA deve essere: *lawful and respectful; purposeful and performance-driven; accurate, reliable and effective; safe, secure and resilient; understandable; responsible and traceable; regulary monitored; transparent; accountable*; sul punto si veda: E. CHITI – B. MARCHETTI, *Divergent? Le strategie di Unione Europea e Stati Uniti in materia di intelligenza artificiale*, cit., 1, 2020, 29.

Inoltre, l'e.o. 13960 incarica il *Federal Chief Information Officer Council* di intraprendere la catalogazione dei sistemi di IA che vengono adoperati dalle agenzie federali[269].

Infine, un terzo gruppo di atti concerne il consolidamento della strategia statunitense contenuta nell'e.o. 13859 con la conversione in legge delle proposte frammentarie dell'Esecutivo.

A tal proposito, il *National Defense Authorization Act for Fiscal Year* 2021 ha istituito il *National AI Initiative Office*, che ha essenzialmente funzioni di impulso e coordinamento ed è incardinato nell'*Office of Science and Technology Policy* della Casa Bianca; inoltre, con lo stesso atto è stata istituita la *National AI Research Resource Task Force*, che è chiamata a svolgere una funzione consultiva a supporto del Presidente e del Congresso; è divenuta operativa con la nomina di dodici esperti provenienti dal settore privato ed ha predisposto una piattaforma (la *National AI Research Resource*) a disposizione dei ricercatori e degli sviluppatori.

A livello settoriale, sono state elaborate varie proposte volte a disciplinare profili specifici dell'IA.

Nel 2021 sono stati due gli atti elaborati e sono relativi all'impiego di sistemi intelligenti sia in ambito militare che a livello di intelligence[270].

---

[269] Si veda: L. PARONA, *"Government by algorithm": un contributo allo studio del ricorso all'intelligenza artificiale nell'esercizio di funzioni amministrative*, in *Giorn. Dir. amm.*, 1, 2021, 10.

[270] I due atti hanno recepito la maggior parte delle raccomandazioni contenute nel report della National Security Commission on AI e stabiliscono norme relative alla formazione,

A maggio 2021, è stato istituito alla Camera l'*Algorithmic Justice and Online Platform Transparency Act of 2021* che al fine di rendere più pervasivo il controllo *ex post*, obbliga i gestori della piattaforma ad illustrare i procedimenti impiegati in modo da renderli conoscibili agli utenti.

Si devono segnalare le iniziative settoriali delle singole agenzie che si inseriscono nell'ambito del *memorandum "Guidance for Regulation of Artificial Intelligence Applications"* del novembre 2020. Il Direttore dell'OMB ha esortato le agenzie ad intervenire con un approccio non regolatorio, quindi tramite *policy* settoriali, progetti pilota, *standards* e *frameworks* volontari.

In tale contesto sono stati avviati vari procedimenti di regolazione che nella maggior parte dei casi sono ancora in una fase iniziale.

Per quanto riguarda la regolazione dei singoli Stati, in molti casi è stata sensibilmente più rapida ed ha comportato l'istituzione di autorità amministrative competenti in materia di intelligenza artificiale e dotate di funzioni consultive.

L'attività legislativa si configura lenta e rigida; pertanto, non idonea a tenere il passo con l'innovazione digitale. Il Congresso ha elaborato normative a carattere amministrativo che istituiscono organismi specializzati e stabiliscono norme di principio.

aggiornamento, assunzione di personale qualificato in materia di IA. La Commissione è stata istituita con il *National Defense Authorization Act for Fiscal Year* 2019.

Nonostante i plurimi sforzi, si deve rilevare che il Congresso non ha adottato soluzioni decisive in materia; in quanto, ha adattato la normativa esistente all'IA ed ha introdotto regole concernenti in modo specifico i sistemi intelligenti (ad esempio, il principio di *explainability* con riferimento agli algoritmi), ma non ha ancora individuato i soggetti responsabili in materia di evoluzione dell'intelligenza artificiale.

Non sono mancati i tentativi di interventi regolatori pubblici, ma le difficoltà riscontrate hanno condotto verso una sostanziale *self-regulation*.

Gli Stati Uniti rispetto all'Europa sembrano intraprendere una politica "più leggera" volta ad incentivare lo sviluppo dell'intelligenza artificiale anche a costo di sacrificare i diritti dei soggetti coinvolti. La politica intrapresa dimostra l'intento americano di non perdere opportunità competitive soprattutto rispetto a paesi come la Cina che hanno adottato nel tempo politiche spregiudicate pur di favorire lo sviluppo tecnologico.

4. La sostenibilità di una *compliance* automatizzata alla luce del quadro normativo europeo.

Il Legislatore europeo – come emerge dalla proposta di regolamento sull'intelligenza artificiale[271] (*Artificial Intelligence Act*) – ha adottato una linea regolatoria adattata al rischio.

[271] Il percorso si è aperto con l'adozione del Libro Bianco sull'IA il 19 febbraio 2020.

L'intento è realizzare una normativa che si conformi alle esigenze di contemperamento degli interessi in gioco, conciliando lo sviluppo tecnologico con la tutela dei diritti fondamentali dei soggetti coinvolti.

La scelta di adottare un Regolamento è rappresentativa dell'intento di realizzare una normativa uniforme, riducendo la possibilità per gli Stati di intervenire in maniera sostanziale sulla disciplina.

L'intera attività normativa che coinvolge i sistemi tecnologici sembra essere "a metà strada" affiancando ad ipotesi fortemente innovative, tendenze conservatrici.

Le misure che si possono definire "progressiste" riguardano ad esempio, l'introduzione di principi giuridici nuovi, quali la trasparenza e la comprensibilità degli algoritmi; la responsabilizzazione dei soggetti privati in termini di *accountability* e la disciplina da adottare in caso di sistemi tecnologici ad alto rischio.

In altri casi sono stati realizzati interventi che ricalcano le tecniche legislative adottate generalmente in ambito europeo; si pensi alla disciplina in materia di sicurezza dei prodotti e dei servizi che adoperano l'IA, che prevede l'adozione di *standard* di sicurezza e di procedure autorizzative per la messa in commercio e per l'esecuzione di controlli da parte dei soggetti specializzati.

In ogni caso, si deve rilevare che l'approvazione della proposta di regolamento sull'IA ha determinato un forte passo avanti verso la regolazione

della materia, ma bisognerà aspettare la conclusione dell'*iter* e l'entrata in vigore per tutti gli Stati membri per valutarne l'efficacia e l'effettività.

CONCLUSIONI

Al termine dell'esposizione si può dire che gli obiettivi della presente ricerca sono stati raggiunti.

Le nuove tecnologie rappresentano uno strumento che si sta sviluppando su più livelli e le cui potenzialità sono tali da far superare le perplessità rispetto ad un utilizzo massivo anche in ambito aziendale.

Le imprese - come è stato osservato - necessitano di conformarsi alle disposizioni normative afferenti a vari settori del diritto. La *compliance*, infatti, assume un ampio respiro rappresentando un metodo di gestione basato sul *risk assestment* e sul *risk managment* che mira a prevenire determinati rischi per evitare che si verifichino eventi contrari alla legge oppure a regole autonormate.

Sebbene la *compliance* assuma un significato molto ampio, il presente lavoro si è focalizzato sulla disciplina di cui al d.lgs. 231 del 2001. Le persone giuridiche con l'introduzione della responsabilità amministrativa dipendente da reato sono chiamate a rispettare una serie di regole per evitare di incorrere in sanzioni che oltre ad essere onerose comportano un forte danno, in termini reputazionali, per l'azienda.

A tal fine, l'adozione di modelli organizzativi idonei a prevenire il rischio di verificazione dei reati presupposto previsti dal d.lgs. 231 del 2001, rappresenta un elemento fondamentale.

Il rimprovero che viene mosso all'azienda si basa sul riconoscimento della c.d. colpa di organizzazione; in altre parole, l'ente ha omesso di adottare le misure che avrebbero potuto evitare la verificazione del reato.

Il problema fondamentale della *compliance* per le imprese riguarda la molteplicità di fonti che spesso ostacolano l'adozione di regole che siano capillari, ma soprattutto aggiornate.

L'impego di tecnologie avanzate risponde proprio alla finalità di assistere l'agente umano nell'attività di *risk assestment* e di *risk management*.

Una completa automatizzazione – come si è visto – è ostacolata dalle difficoltà di imputazione della responsabilità in caso di errore della macchina dovuta principalmente al passaggio da sistemi esperti a sistemi intelligenti.

L'ipotesi di un'imputazione diretta dell'agente artificiale - sebbene sia suggestiva - presenta molteplici criticità, dettate dal fatto che se da un lato, la macchina è capace nelle sue forme più avanzate di autoapprendere dall'altro, non ha la capacità di pensare e di autodeterminarsi; quindi, una diretta responsabilizzazione della stessa contrasterebbe con lo schema di imputazione previsto nel nostro ordinamento che richiede la presenza di comportamento riferibile al soggetto in termini oggettivi e soggettivi.

Nel corso del lavoro è stato evidenziato che anche la previsione di una responsabilità diretta per i soggetti umani che interagiscono con la macchina (programmatori, produttori, utilizzatori) non è ipotizzabile – soprattutto per gli agenti artificiali che si basano sui meccanismi di *machine learning* –

poiché, si tratterebbe di una responsabilità per fatto altrui determinata dal *deficit* di *explainability* che caratterizza la maggior parte dei sistemi artificiali.

Come si è visto, la soluzione del *responsability gap* è ancora lontana, però soprattutto a livello europeo la strada della regolamentazione potrebbe rappresentare una svolta che consentirebbe di bilanciare le esigenze di sviluppo con quelle di tutela degli interessi dei soggetti coinvolti.

Il lavoro è stato incentrato principalmente sullo studio dell'intelligenza artificiale e della *blockchain* poiché risultano essere le tecnologie che hanno avuto un ampio sviluppo in tutti i settori compreso quello giuridico.

La *blockchain* ha iniziato ad essere utilizzata nel settore finanziario dove la garanzia di trasparenza, tracciabilità delle operazioni, disintermediazione e di sostanziale immodificabilità dei dati inseriti ne hanno incentivato la diffusione.

Anche l'intelligenza artificiale e più in generale gli strumenti tecnologici hanno avuto un rapido sviluppo nel settore finanziario e bancario proprio per il tipo di operazioni che vengono realizzate e per i benefici che potevano derivarne in termini di velocizzazione e di sicurezza delle transazioni.

A livello aziendale è fondamentale rispondere all'esigenza di gestire un'enorme massa di dati; pertanto, l'utilizzo di sistemi automatizzati per la gestione dei processi, la mappatura delle aree a rischio reato e l'analisi dei flussi informativi costituisce un elemento fondamentale che contribuisce a garantire l'efficienza della stessa azienda.

Si è visto però, che l'utilizzo dei sistemi intelligenti o della c.d. catena dei blocchi non è da solo sufficiente a gestire le attività corporative e nello specifico a prevenire la verificazione del rischio in ambito penale, ma è necessario che permanga l'intervento umano quantomeno nella fase di controllo delle attività e dei procedimenti.

Invero, l'utilizzo dell'Intelligenza artificiale e della *blockchain* mette a rischio la tutela dei diritti fondamentali dei soggetti coinvolti.

Ad esempio, per quanto riguarda i dati personali che vengono trattati nei sistemi che adoperano la *blockchain* e l'IA i principi di esattezza dei dati, di aggiornamento, di minimizzazione e di adeguatezza espressi dalla normativa e dal Regolamento sulla protezione dei dati personali non consentono di reperire dati come se si eseguisse una "pesca a strascico" senza avere chiari gli obiettivi e non considerando la correttezza e l'esattezza dei dati.

L'analisi casistica condotta - anche se non può dirsi esaustiva - ha proprio lo scopo di dimostrare quale sia l'utilità dello strumento tecnologico per l'individuazione di attività illecite (quali ad esempio, l'esfiltrazione di dati, le frodi oppure l'accesso abusivo a sistema informatico).

Dal punto di vista normativo, l'Unione Europea, rispetto ad altre potenze mondiali, preferisce la strada della regolamentazione con l'adozione di un'unica linea di indirizzo; ciò è dimostrato dalla scelta del Regolamento per disciplinare l'Intelligenza artificiale.

In conclusione, si può affermare che - nonostante la materia sia in rapida evoluzione e quindi necessiti di uno studio costante e di continui

aggiornamenti - l'obiettivo della presente ricerca può dirsi raggiunto in quanto, si è dimostrato che la tecnologia può avere un ruolo fondamentale nell'attività di *criminal compliance* a livello aziendale consentendo un'analisi dei dati e delle attività che sia capillare ed efficiente ed effettui un adeguato bilanciamento degli interessi dei soggetti coinvolti.

BIBLIOGRAFIA

R. ABBOT - A. SARCH, *Punishing Artificial Intelligence: Legal Fiction or Science Fiction*, in *UC Davis Law Review*, 2019, 53, 355 ss.

N. ABRIANI - G. SCHNEIDER, *Diritto delle imprese e intelligenza artificiale*, Bologna, 2021, 123 ss.

N. ABRIANI, *Successo sostenibile e regole statutarie: il ruolo del board nel Codice di Corporate Governance*, in *"Rivista di Corporate Governance",* I, 2021, 17-18.

N. ABRIANI - F. GIUNTA, *L'organismo di vigilanza previsto dal d. lgs. 231/2001. Compiti e funzioni*, in *Rivista 231*, 2012, III, 191 ss.

N. ABRIANI, *La responsabilità da reato degli enti: modelli di prevenzione e linee evolutive del diritto societario*, in *Analisi giuridica dell'economia*, 2012, 198.

A. ALESSANDRI, *Diritto penale e attività economiche*, Bologna, 2010, 225.

A. ALESSANDRI, *La vocazione penalistica dell'ODV e il suo rapporto con il modello organizzativo*, in AA. VV., *I controlli societari*, 442.

G. ALPA, *FinTech: un laboratorio per i giuristi*, in *Contr. Impr*., 2019, 378.

S. ALVARO – L. MARZIALETTI – D. TUZZOLINO, *Evoluzioni normative fra policy e diritto*, in *La portabilità dei dati in ambito finanziario*, a cura di A. GENOVESE e V. FALCE, in *Quaderni FinTech*, www.consob.it.

G. AMATO, *Il modello di organizzazione nel sistema di esonero dalla responsabilità: ragioni di una scelta prudenziale*, in *Resp. amm. soc. enti*, 2015, 2, 55 ss.

C. AMATO, *La computerizzazione del* contratto *(smart, data oriented, computable e self-drivingcontract. Una panoramica)*, in *Eur. Dir. priv*., 2020, 1268.

A. AMIDEI, *Intelligenza artificiale e product liability: sviluppi del diritto dell'Unione Europea*, in *Giur. It*., 2019, 1715.

R. AMIT – C. ZOTT, *Value creation in e-business. Strategic management journal*, vol. 22, n. 6-7, 493-520; L. LI – F. SU – W. ZHANG – J. Y. MAO, *Digital transformation by SME enterpreneures: A* capability perspective, in Information Systems Journal, vol. 28, n. 6, 2018, 1129-1157.

C. APPETITI, *Il sistema di compliance di UniCredit*, in ROSSI, *La corporate compliance: una nuova frontiera per il diritto?*, Milano, 2017, 51.

J. ARLEN, *The Law of Corporate Investigations and the Global Expansion of Corporate Criminal Enforcement*, in *S. Cal. L. Rev*., 2020, 93, 699 ss.

P. M. ASARO, *A body to kick, but Still No Soul to Damn: Legal Perspective on Robotics*, in LIN, ABNEY, BEKEY, *Robot Ethics*, Cambridge, 2012, 169 ss.

P. M. ASARO, *Determinism, machine agency, and responsibility*, in *Politica e società*, 2014, 282 ss.

V. ATTILI, *L'agente-modello "nell'era della complessità": tramonto, eclissi o trasfigurazione?*, in *Riv. It. Dir e proc. pen*., 2006, 4, 1240 ss.

M. ATZORI, *Blockchain Technology and Decentralized Governance Is the State Still Necessary?*, in *Ssrn.com*, 2 gennaio 2016.

A. AVITABILE, *Il data protection officer*, in G. FINOCCHIARO, (a cura di) *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, 2017.

A. AZARA, *Intelligenza artificiale e personalità giuridica*, in *Il diritto nell'era digitale*, a cura di R. GIORDANO, A. PANZAROLA, A. POLICE, S. PREZIOSI, M. PROTO, Milano, 2022, 91 ss.

A. BALDASSARRE, *Diritti della persona e valori costituzionali*, Torino, 1997, 57 ss.

R. BARTOLI, *Il criterio di imputazione oggettiva*, in G. LATTANZI, P. SEVERINO *(a cura di), Responsabilità da reato degli enti*, vol. I, Torino, 2020, p. 186 ss.

F. BASILE, *Intelligenza artificiale e diritto penale: quattro possibili percorsi d'indagine*, in *Diritto Penale e Uomo*, 29 settembre 2019, 27 ss.

M. BASSINI, L. LIGUORI, O. POLLICINO, *Sistemi di Intelligenza artificiale, responsabilità e accountability. Verso nuovi paradigmi?*, in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Milano, 2018, 363 ss.

R. BATTAGLINI, *La normativa italiana sugli smart contract*, in *Blockchain e smart contract*, Milano, 2019, 375.

E. BATTELLI, *Diritto privato digitale*, Milano, 2022, 261 ss.; P. BOUCHER, *Come la tecnologia blockchain può cambiarci la vita*, trad. it., Bruxelles, 2017, 15 ss.

S. J. BEALE, P. BERRIS, *Hacking the Internet of Things: Vulnerabilities, Dangers, and Legal Responses*, in *Duke Law & Technology Review*, 2017-2018, 16, 161 ss.

U. BECHINI – M. C. CIGNARELLA, *Antiriciclaggio – compravendita di immobile – pagamento del prezzo in bitcoin, Quesito antiriciclaggio n. 3/2018*, in *Not*., 20 marzo 2018.

T. BELARDI, *Gli smart contract: storia e definizioni di un ibrido contratto/software*, in *Blokchain e smart contract*, Milano, 2019, 225 ss.
M. BELLACOSA, *Il luogo di consumazione del delitto di accesso abusivo a un sistema informatico o telematico: in attesa delle Sezioni unite*, in *Dir. Pen. Cont*., 2 febbraio, 6, 2015.

A. BERNASCONI, *Art. 6*, in A. PRESUTTI – A. BERNASCONI – C. FIORIO, *La responsabilità degli enti*, Padova, 2008, 118; G. ZANALDA – M. BARCELLONA, *Responsabilità amministrativa delle società*, Milano, 2002, 72.

A. BERTOLINI, *Robot as Products: The case for a realistic analysis of robotic applications and liability rules*, in *Law Innovation and Technology*, 2013, 5,3, 214 ss.

E. BERTOLLI, *L'organismo di vigilanza ex d. lgs. 231/2001 nella dottrina e nella giurisprudenza*, in *Rivista 231*, 2010, I, 61.

V. B. BHARGAVA, M. VELASQUEZ, *Is corporate responsibility relevant to Artificial Intelligence Responsibility?*, in *The Georgetown Journal of Law Public Policy*, 2019, 17, 830 ss.

E. BIRRITTERI, *Big Data Analytics e compliance anticorruzione. Profili problematici delle attuali prassi applicative e scenari futuri*, in *Dir. pen. cont.*, 2, 2019, 295 ss.

R. BODEI, *Dominio e sottomissione*, Bologna, 2023, 333.

M. A. BOEDEN, *Artificial Intelligence. A Very Short introduction*, Oxford, 2018.

L. BOLOGNINI – E. PELINO – C. BISTOLFI, *Il regolamento privacy europeo*, Milano, 2018.

R. BORSARI, *Intelligenza artificiale e responsabilità penale: prime considerazioni*, in *Rivista del diritto dei media*, 2019, 3, 262 ss.

N. BOURTIN - A. HOULE, *Investigazioni interne: uno sguardo all'esperienza americana*, in CENTONZE – MANTOVANI, *La responsabilità penale degli enti: dieci proposte di riforma*, Bologna 2016, 199.

P. BRAMBILLA, *Disastro ferroviario di Viareggio: le motivazioni della sentenza della Cassazione*, in Riv. Sistema Penale, 2021.

P. J. BRANTINGHAM, *The Logic of Data Bias and Its Impact on Place-Based Predictive Policing*, in *Ohio State Journal of Criminal La*w, 2018, 473.

K. BRENNAN-MARQUEZ, *Big Data policing and the Redistribution of Anxiety*, in *Ohio State Journal of Criminal Law*, 2018, 487.

F. BRICOLA, *Il costo del principio "societas delinquere non potest" nell'attuale dimensione del fenomeno societario*, in *Riv. Trim. dir. proc. pen.*, 1970, 951 ss.

C. BURCHARD, *Digital criminal compliance*, in *Digitalisierung, Globalisierung und Risikoprävention. Ferschrift für Ulrich Sieber zum 70. Geburstag*, a cura di ENGELHART – KUDLICH – VOGEL, Berlin, 2021, 741 ss.

C. BURCHARD, *L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società,* Riv. It. Dir. Proc. pen., 2019, 17.

J. BURREL, *How the machine "thinks": Understanding opacity in machine learning algorithms,* in *Big Data & Society*, 2016, n. 3, 1 ss.

V. BUTERIN, *A next generation smart contract and decentralized application platform*, Ethereum White Paper, disponibile online.

A. CADOPPI, C. M. PRICOLO, *Strict Liability nel diritto anglo-americano (voce)*, in *Dig. Pen*., vol. XIV, Torino, 1999, 20 ss.

R. CALÒ, I. EVTIMOV, E. FERNANDS ET AL., *Is Tricking a Robot Hacking?*, in *Berkeley Technology Law Journal*, 2019, 34, 891 ss.

R. CALÒ, *Robotics and the Lesson of Cyberlaw*, in *California Law Rewiew*, 2016.

M. F. CAMPAGNA, *Gli scambi attraverso algoritmi e il problema del linguaggio*, in *Rivistawe*b, 1, 2019, 3.

S. CAMPANELLA, *Profili problematici in tema di documenti dichiarativi*, IP, 2008, 162.

S. CAPACCIOLI, *Criptovalute e bitcoin. Un'analisi giuridica*, Milano, 2015, 21.

A. CAPELLINI, *Machina delinquere non potest? Brevi appunti su intelligenza artificiale e responsabilità penale*, in Criminalia, 2018, 499 ss.

A. CAPELLINI, *Profili penalistici delle self-driving cars*, in *Dir. Pen. Cont*., 2019, 2, 335 ss.

A. CAPOGNA - L. PERAINO - S. PERUGI - M. CECILI - G. ZBROWSKI - A. RUFFO, *Bitcoin: profili giuridici e comparatistici. Analisi e sviluppi futuri di un fenomeno in evoluzione*, in *Di.m.t.*, 2015, in nota 23.

M. CAPUTO, *La mano visibile. Codici etici e cultura d'impresa nell'imputazione della responsabilità degli enti*, in *Dir. pen. cont. – Riv. Trim*., 1/2013, 114.

D. CARBONI, *Le tecnologie alla base della blockchain*, in *Blockchain e smart contract*, Milano, 2019, 33 ss.

S. CAVALLINI, *Il giudizio di idoneità dei modelli organizzativi: barlumi di. Colpa nell'eterno meriggio della responsabilità in re ipsa dell'ente?*, in *Resp. amm. soc. enti*, 2015, 4, 159.

F. CENTONZE – M. MANTOVANI, *La responsabilità penale degli enti: dieci proposte di riforma*, Bologna, 2016, 288.

F. CENTONZE, *Controlli societari e responsabilità penale*, Giuffrè, 2009, 412.

F. CENTONZE, *Responsabilità da reato degli enti e "agency problems". I limiti del d.lgs. n. 231 del 2001 e le prospettive di riforma*, in *Riv. It. Dir. e proc. pen*, 2017, 946 ss.

R. CLARIZIA – E. NATI, *La responsabilità amministrativa delle persone giuridiche: il d. lgs. 231/01 tra principi generali dell'ordinamento e nuovi organi societari*, in *Giur. Comm.*, 2002, 306.

G. COLÒ, *"Anomaly detection for Cyber Security: Time Series Forecasting and Deep Learning", International Journal of Scientific Research in Mathematical and Statistical Sciences*, Vol.7, Issue.1, 2020, 40-52.

F. CONSULICH, *Il nastro di Mobius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso di mercato*, in *Banca borsa titoli di credito*, 2018, 2, 195-234.

L. D'AGOSTINO, *La tutela penale dei dati personali nel riformato quadro normativo: un primo commento al D.Lgs. 10 agosto 2018, n. 101*, in *Archivio pena*le, 2018, 1-58.

F. D'ARCANGELO, *Il sindacato giudiziale sui modelli organizzativi nel contesto attuale*, in R. BORSARI (a cura di), *Itinerari di diritto penale dell'economia*, p. 351 ss.

L. S. DALENOGARE - G. B. BENITEZ - N. F. AYALA – A. G. FRANK, *The expected contribution of Industry 4.0 technologies for industrial performance*, in *International Journal of Production Economics*, vol. 24, 2018, 383-394.

G. DALIA, *L'esperienza italiana nella lotta alla corruzione: prevenzione, sanzione penale, contrasto processuale e performance*, in *Iura and legal systems*, n. 4/2019, 27-31.

J. DANAHER, *Robots, Law and the Retribution Gap*, in *Ethics and Information Technology*, 2016, 18,4, 299 ss.

C. DE MAGLIE, *L'etica e il mercato. La responsabilità penale della società*, Giuffrè, 2002.

A. DE NICOLA, *Il diritto dei controlli societari*, Milano 2010, 91 ss.

A. DE NICOLA, *L'organismo di vigilanza 231 nella società di capitali*, Torino, 2015.

G. DE SIMONE, *I profili sostanziali della responsabilità amministrativa degli enti: la "parte generale" e la "parte speciale" del d.lgs. 8 giugno 2001 n. 231*, in AA. VV., *Responsabilità degli enti per illeciti amministrativi dipendenti da reato*, Cedam, 2002, 73 ss.

G. DE SIMONE, *La responsabilità da reato degli enti nel sistema sanzionatorio italiano: alcuni aspetti problematici*, in *Riv. Trim. dir. pen. econ.*, 2004, 675.

G. DE SIMONE, *Persone giuridiche e responsabilità da reato. Profili storici, dogmatici e comparatistici*, *Edizioni ETS*, 2012, 182 ss.

G. DE SIMONE, *Societas delinquere et puniri potest, La questione della responsabilità penale degli enti collettivi tra dogmatica e politica criminale*, Como, 2000, 203 ss.

G. DE VERO, *La responsabilità penale delle persone giuridiche*, Milano, 2008, 311 ss.

G. DI GARBO – F. GAUDINO – E. M. MANCUSO – M. VASILE, *Italy*, in SPEHL – GRUETZNER, *Corporate internal investigation*, München, 2012, 248.

O. DI GIOVINE, *Lineamenti sostanziali del nuovo illecito punitivo*, in (a cura di G. LATTANZI) Reati e responsabilità degli enti, Giuffrè, 2010, 3 ss.

F. DI MAIO, *Prevenzione e dissuasione dei reati informatici nel modello organizzativo*, in *Cybercrime e responsabilità da reato degli enti: prevenzione, modello organizzativo e indagini preliminari* (a cura di) ANDREA MONTI, Milano, 2022, 149 ss.

D. DOUGHERTY – D. DUNNE, *Digital science and Knowledge boundaries in complex innovation. Organization Science*, Vol. 23, n. 5, 1467-1484.

J. DREXL, R.M. HILTY ET AL., *Technical Aspects of Artificial Intelligence: An Understanding from an Intellectual Property Law Perspective*, Version 1.0, ottobre 2019, 8.

R. DUIZONI, *Mappatura di aree a rischio e formazione della relativa documentazione dimostrativa dei passi compiuti da offrire al giudice o al pubblico ministero quale attività ex 391-nonies c.p.p. attività investigativa preventiva*, in www.rivista231.it.

L. A. ENRIQUES - D.A. ZETZSCHE, *Corporate technologies and the Tech Nirvana Fallacy*, 2019, 19.

L. ENRIQUES, *Financial Supervisors and RegTech: Four Roles and Four Challenges*, in *"RTDF"*, 2017, 53 ss.

N. FABIANO, *The Internet of Things ecosystem: the blockchain and privacy issues. The challenge for a global privacy standard Advances*, in *Science, Technology and Enginnering Systems Journal*, vol. 3, n. 2, 2018, 5.

P. FERRUA, *Il processo penale contro gli enti: incoerenze ed anomalie nelle regole di accertamento*, in G. GARUTI (a cura di), *Responsabilità degli enti per illeciti amministrativi dipendenti da reato*, Padova, 2002, 232.

G. FIDELBO – R. A. RUGGIERO, *Procedimento a carico degli enti e messa alla prova: un possibile itinerario*, www.rivista231.it, 2016, 14.

A. FIORELLA, *Il trasferimento di funzioni nel diritto penale*, Nardini, 1985.

G. FLORA, *Le sanzioni punitive nei confronti delle persone giuridiche: un esempio di metamorfosi della sanzione penale?*, in *Dir. pen e proc*., 2003, 1398 ss.

V. L. FOFFANI, *Genesi e sviluppo (e prospettive future) di un modello di responsabilità degli enti nell'Unione Europea*, in D. PIVA (a cura di), *La responsabilità degli enti ex d. lgs. n. 231/2001 tra diritto e processo*, Torino, 2021, 26 ss.

P. M. FREITAS, F. ANDRADE, P. NOVAIS, *Criminal Liability of Autonomous Agent: From the Unthinkable to the Plausible*, in CASANOVAS-PAGALLO-PALMIRANI-C. FRIGENI, C. PRESCIANI, *L'organismo di vigilanza*, in *Compliance. Responsabilità da reato degli enti collettivi*, (a cura di) D. CASTRONUOVO, G. DE SIMONE, E. GINEVRA, A. LIONZO, D. NEGRI, G. VARRASO, Milano, 2019, 262.

A. GARAPON-LASSAGUE, *La giustizia digitale*, Bologna, 2021, 111-112.

A. GARGANI, *Posizioni di garanzia nelle organizzazioni complesse: problemi e prospettive*, in *Riv. Trim. dir. pen. econ.*, 2017, 508 ss.

G. GASPARRI, *Timidi tentativi giuridici di messa a fuoco del Bitcoin: miraggio monetario criptoanarchico o soluzione tecnologica in cerca di un problema?*, in *Dir. Inform.*, 2015, 415 ss.

S. GLESS, E. SILVERMAN, T. WEIGEND, *If Robots Cause Harm, who is to blame? Self-driving cars and criminal liability*, in *New Criminal Law Review*, 2018, 677 ss.

B. P. GOECKE, *Artificial Intelligence*, Padeborn, 2020; P. WANG, *On Defining Artificial Intelligence*, in *Journal of Artificial Intelligence*, 10, 2017, 1.

C. GROSSO, voce *Responsabilità penale*, in *Nss. Dig. It.*, Utet, vol. XV, 1968, 712.

A. GULLO, *I modelli organizzativi*, cit., in G. LATTANZI, P. SEVERINO *(a cura di), Responsabilità da reato degli enti*, vol. I, Torino, 2020, 244 ss.

A. GULLO, *La responsabilità dell'ente e il sistema dei delitti di riciclaggio*, in AA. VV., *Diritto penale dell'economia*, diretto da CADOPPI-CANESTRARI-MANNA-PAPA, t. II, Utet, 2019.

K. GÜNTHER, *Bedrothe individuelle Freihithen im aufgelärten Strafrecht – Welche Freiheiten?*, in *KJ*, 2016, 250.

G. HALLEVY, *Liability for Crimes Involving Artificial Intelligence System*, 2015.

J. HAN, Y. HUANG, S. LIU et al. *Artificial intelligence for anti-money laundering: a review and extension.* Digit Finance 2, 211–239 (2020).

K. J. HAYWARD, M. M. MAAS, *Artificial Intelligence and crime: A primer for criminologist*, in *Crime Media Culture*, 2020, 7 ss.

R. HEDENDEHL, *Corporate Criminal Liability: Model Penal Code Section 2.07 and the Development in Western Legal Systems*, in *Buff. Crim*. L. R., 2000, 4, 283 ss.

S. E. HENDERSON, *A Few Criminal Justice Big Data Rules,* in *Ohio State Journal of Criminal Law*, 2018, 527.

M. HILDEBRANDT, *Autonomic and autonomous thinking. Preconditions for criminal accountability*, in *Hildebrandt, Rouvroy, Law, Houman Agency and Autonomic Computing*, Abingdon, 2011, 141 ss.

E. HIGENDORF, *Autonome Systeme, Künstliche Intelligenz und Roboter*, in AA. VV. (a cura di S. BARTON ET AL.), *Festschrift für Thomas Fisher*, C. H. BECK, 2018, 111 ss.

E. HILGENDORF, *Automated Driving and the Law*, in E. HILGENDORF, U. SEIDEL (a cura di), *The Law*, Baden-Baden, 2017, 181 ss.

J. HORDER, *Ashworth's Principles of criminal law*, 9th ed., 2019, 181.

D. IACOVENE, *La trasformazione dei modelli di business nell'era digitale*, Bologna, 2018.

P. IELO, *Autoriciclaggio e responsabilità dell'ente ex d.lgs. 231/2001*, in MEZZETTI, PIVA, *Punire l'autoriciclaggio. Come, quando e perché*, Torino, 2016, 50 ss.

P. IELO, *Compliance programs: natura e funzione nel sistema della responsabilità degli enti. Modelli organizzativi ex d.lgs. 231/2001*, in *Resp. amm. soc. enti*, 2006, 1, 99 ss.

T. C. KING, N. AGGARWAL, M. TADDEO, L. FLORIDI, *Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions*, in *Science and Engineering Ethics*, 2020, 26, 94 ss.

F. LAGIOIA, G. SARTOR, *AI system under Criminal Law: a Legal Analysis and a Regulotary Perspective*, in *Philosophy Tecnology*, 2019, 1 ss.

M. LAMO, R. CALO, *Regulating Bot Speech*, in U.C.L.A. *Law Rewiew*, 2019, 988, 66.

D. C. LANGEVOORT, *Global Behavioral Compliance*, in *Corporate on a Global Scale, in Corporate Compliance on a Global Scale*, 2022, 217-236., 217.

G. LATTANZI, *Introduzione,* in AA. VV., *Responsabilità degli enti per illeciti amministrativi dipendenti da reato*, Cedam, 2002, 1 ss.

G. LATTANZI, *Intervento*, in AA. VV. (a cura di PALAZZO), Societas puniri potest, 291.

W. LAUFER, *Inautenticità del sistema della responsabilità degli enti e giudizio di colpevolezza*, in AA. VV., *La responsabilità penale degli enti*, 11.

F. LEDDA, *I protocolli dei Modelli Organizzativi*, in www.rivista231.it.

F. LI – A. NUCCIARELLI – S. RODEN – G. GRAHAM, *How smart cities transform operations models: A new research agenda for operations management in the digital economy*, in *Production Planning e Control*, vol. 27, n. 6, 514-528.

M. LILLÀ MONTAGNANI, *Flussi informativi e doveri degli amministratori di società per azioni ai tempi dell'intelligenza artificiale*, in *Riv. Persona e mercato*, 2, 2020.

D. LIMA, *Could AI agents be held criminally liable? Artificial Intelligence and the Challenges for criminal law*, in *South Carolina Law Review*, 2018, 69, 3, 682 ss.

C. LOEBBECKE – A. PICOT, *Reflections on societal and business model transformation arising from digitization and big data analytics: A research agenda*, in *Journal of Strategic information Systems*, vol. 24, n. 3, 149-167.

MAGRO, *Decisione umana e decisone robotica. Un'ipotesi di responsabilità da decisone robotica*, in *La Legislazione penale*, 10 maggio 2020, 3 ss.

S. MANACORDA, *L'idoneità preventiva dei modelli di organizzazione nella responsabilità da reato degli enti: analisi critica e linee evolutive*, in *Riv. Trim. dir. pen. econ.*, 2017, 71.

R. MANCINI, *L'intelligenza artificiale nel credit scoring finanziario e assicurativo*, in *XXVI lezioni di diritto dell'intelligenza artificiale*, a cura di U. RUFFOLO, 2021, 706 ss.

E. M. MANCUSO, *L'acquisizione di contenuti e-mail*, in SCALFATI, *Le indagini atipiche*, Torino, 2014, 256.

E. M. MANCUSO, *Le investigazioni interne nel procedimento a carico dell'ente*, in D. CASTRONOVO – G. DE SIMONE – E. GINEVRA – A. LIONZO – D. NEGRI – G. VARRASO, *Compliance. Responsabilità da reato degli enti collettivi*, 2019, 1935 ss.

E. M. MANCUSO, *Le investigazioni interne nel sistema processuale italiano: tra vuoto normativo e prassi applicative incerte*, in CENTONZE-MANTOVANI, *La responsabilità penale degli enti: dieci proposte di riforma*, Bologna, 2016, 217.

V. MANES, A. F. TRIPODI, *L'idoneità del modello organizzativo*, in F. CENTONZE – M. MANTOVANI (a cura di), *La responsabilità "penale" degli enti*, 2016, Bologna, 141 ss.

V. MANES, *Profili di metodo nell'accertamento dell'idoneità del modello organizzativo*, in R. BORSARI (a cura di), *Itinerari di diritto penale dell'economia*, 2018, Padova, 337.

Cass. Pen. sez. VI, 15 febbraio 2022, dep. 10 maggio 2022, n. 18413, con nota di L. APUZZO, in *Riv. Trim. dir. pen. ec*., 2022, 363 ss.

A. MANTELERO, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva*, in G. FINOCCHIARO, (a cura di) *Il nuovo Regolamento Europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017.

M. MANTOVANI – L. FRANCESCHINI, *La compliance in ENI*, in *La corporate compliance: una nuova frontiera per il diritto?*, Milano, 2017, 1.

F. MANTOVANI, *Diritto alla riservatezza e libera manifestazione del pensiero*, Milano, 1970, 29 ss.

D. MANZIONE, *La responsabilità amministrativa delle persone giuridiche: una soluzione opportuna o solo di "comodo"?,* in AA.VV. (a cura di G. DE FRANCESCO). *La responsabilità degli enti: un nuovo modello di giustizia "punitiva",* Giappichelli 2002, 97 ss.

G. MARINUCCI, *"Societas puniri potest": uno sguardo sui fenomeni e sulle discipline contemporanee*, in *Riv. Trim. dir e proc. pen*., 2003, 1193 ss.

G. MARINUCCI, *Il reato come azione. Critica di un dogma*, Giuffrè, 1971, 175 ss.

G. MARINUCCI, *Innovazioni tecnologiche e scoperte scientifiche costi e tempi di adeguamento delle regole di diligenza*, in *Riv. It. Dir. e proc. pen*., 2005, 29 ss.

A. MATTHIAS, *The responsibility gap: Ascribing responsibility for the actions of learning automata,* in *Ethics and Information Technology*, 2004, 6, 175 ss.

O. MAZZA, *Fascicolo del difensore e utilizzabilità delle indagini difensive,* in *Giur. It.*, 2002, 1758.

F. MAZZACUVA, *"Deferred prosecution agreements": riabilitazione "negoziata per l'ente collettivo indagato. Analisi comparata dei sistemi di area anglo-americana*, in *Ind. pen.*, 2013, 737 ss.

F. MAZZACUVA, *La diversione processuale per gli enti collettivi nell'esperienza anglo-americana,* in *Dir. pen. cont. – Riv. Trim.*, 2016, 2, 80 ss.

J. MCCARTHY, *What Is Artificial Intelligence, rapp. Tecn.*, Stanford University, 2007.

BARRY F. MCNEIL – D. BRAIN, *Internal Corporate Investigations*, Chicago, 2007, 11.

E. MIK, *Smart contracts: Terminology, technical limitations and real world complexity*, in *Law, Innovation & Technology*, 2017, 1 ss.

G. MOLINARO, *Sono tassabili le manifestazioni di capacità economica emergenti nelle operazioni relative al bitcoin?*, in *Corr. Trib.*, 2018, 2447.

V. MONGILLO, *Il giudizio di idoneità del modello di organizzazione ex d.lgs. 231/2001: incertezze dei parametri di riferimento e prospettive di soluzione*, in *Resp. amm. soc. enti*, 2011, 3, 69 ss.

V. MONGILLO, *Imputazione oggettiva e colpa tra "essere" e normativismo: il disastro di Viareggio*, in *Giur. It.*, 2022, 953 ss.

V. MONGILLO, *L'organismo di vigilanza nel sistema della responsabilità da reato dell'ente: paradigmi di controllo, tendenze evolutive e implicazioni penalistiche*, in *Resp. amm. soc. enti*, 2015, 4, 83 ss.

V. MONGILLO, *Presente e futuro della compliance penale*, in *Sist. Pen.*, 11 gennaio 2022, p. 1 ss.

J. MOORE, *Corporate Culpability Under the Federal Sentencing Guidelines*, *Arizona Law Review*, vol. 34, 1992, 764 ss.

G. MORGANTE, G. FIORINELLI, *Promesse e rischi della compliance penale digitalizzata*, in *Archivio penale*, 2022, 10 ss.

G. D. MOSCO, *Roboboard. L'intelligenza artificiale nei consigli di amministrazione*, in *Riviste Web*, 247-260.

E. MUSCO, *Le imprese a scuola di responsabilità tra pene pecuniarie e misure interdittive*, in *Dir. e Giust*. 2001, p. 23, 8.

N. NAFFINE, *Who are Law's Persons? From Cheshire Cats to Responsabile Subjects*, in *Modern law Review*, 2003, 1, 346 ss.

S. NAKAMOTO, *Bitcoin: A Peer-to-Peer Eletronic Cash System*, in https://bitcoin.com.

A. NATALE, *Intelligenza artificiale e finTech: profili di responsabilità*, Milano, 2022, 43 ss.

G. NEFF, P. NAGY, *Talking to Bots: Symbiotic Agency and the Case of Tay, in International Journal of Communication*, 2016, 10, 4915.

A. NIETO MARTÌN, *Internal investigation, Whistle-Blowing, and Cooperation: The Struggle for Information in the Criminal Process*, in MANACORDA – CENTONZE – FORTI, *Preventing corporate corruption. The Anti-Birbery Compliance Model*, Cham-Heidelberg, 2014, 69.

A. NISCO, *Riflessi della compliance digitale in ambito 231*, in *Sist. Pen.*, 14 marzo 2022, p. 1 ss.

O'SHIELDS, *Smart Contracts: Legal Agreements for the Blockchain*, in *N.C. Banking Inst*. 177, 2017, 190.

T. PADOVANI, *Il nome dei principi ed il principio dei nomi: la responsabilità amministrativa delle persone giuridiche*, in AA. VV. (a cura di G. DE FRANCESCO), *La responsabilità degli enti: un nuovo modello di giustizia punitiva*, Giappichelli 2004, 13 ss.

U. PAGALLO, *The Laws of Robots. Crimes, Contracts, Torts*, Dordrecht, 2013, 45 ss.

M. PAGANI - C. PARDO, *The impact of digital technology on relationships in a business network*, in *Industrial Marketing management*, vol. 67, 185-192.

C. E. PALIERO - C. PIERGALLINI, *La colpa di organizzazione*, in *La responsabilità amministrativa delle società e degli enti*, 2006, 167 ss.

C. E. PALIERO, *Colpa di organizzazione e impresa*, in M. DONINI, R. ORLANDI (a cura di), *Reato colposo e modelli di responsabilità*, Bologna, 2013, 161 ss.

C. E. PALIERO, *La colpa di organizzazione tra responsabilità collettiva e responsabilità individuale*, in *Riv. Trim. dir. pen. ec.*, 2018, 175 ss.

C. E. PALIERO, *La società punita del perché, del per come, del per cosa*, in *Riv. It. Dir. proc. pen*., 2008, 1516 ss.

C. E. PALIERO, *Problemi e prospettive della responsabilità penale dell'ente nell'ordinamento italiano*, in *Riv. Trim. dir. e proc. pen.*, 1996, 1175.

C. E. PALIERO, *Responsabilità degli enti e principio di colpevolezza al vaglio della cassazione: occasione mancata o definitivo de profundis?*, in *Soc.*, 2014, 4, 474 ss.

M. PANASITI, *sub. Art. 17*, in LEVIS-PERINI, *La responsabilità amministrativa delle società e degli enti,* Bologna, 2014, 356.

B. PANATTONI, *Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'autonomia artificiale,* in *Dir. dell'informazione e dell'informatica*, II, 317 ss.

C. PECORELLA, *Principi generali e criteri di attribuzione della responsabilità*, in A. ALESSANDRI e AL. (a cura di), *La responsabilità amministrativa degli enti D. lgs. 8 giugno 200, n. 231*, p. 82 ss.

C. PEDRAZZI, *Corporate governance e posizioni di garanzia: nuove prospettive?*, in AA. VV., *Governo dell'impresa e mercato delle regole. Scritti giuridici per Guido Rossi, II*, Giuffrè, 2002, 1375.

C. PEDRAZZI, *Profili problematici del diritto penale d'impresa*, in *Riv. Trim, dir. pen. econ*., 1988, 140 ss.

M. PELISSERO, *Responsabilità degli enti*, in F. ANTOLISEI, *Manuale di diritto penale. Leggi complementari*, a cura di A. ROSSI, vol. II, 15° ed., Milano, 2022, 881 ss.

G. PERLINGIERI, *Profili applicativi della ragionevolezza nel diritto civile*, Napoli, 2015.

A. PERNA, *Le origini della blockchain*, in *Blockchain e smart contract*, Milano, 2019.

L. PIATTI, *Dal codice civile al codice binario: blockchain e smart contracts*, in *Cyberspazio e diritto*, 2016, 337.

L. PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in *Cybercrime*, Milano, 2019, 39 ss.

L. PICOTTI, *Reati informatici, riservatezza, identità digitale*, contributo AIPDP, 1 ss.

C. PIERGALLINI, *Danno da prodotto e responsabilità penale, Profili dogmatici e politico-criminali*, Milano, 2004, 12 ss.

C. PIERGALLINI, *Intelligenza artificiale: da 'mezzo' a 'autore' del reato?*, in *Riv. Italiana di diritto e procedura penale*, 4, 2020, 1745 ss.

C. PIERGALLINI, *La struttura del modello di organizzazione, gestione e controllo del rischio-reato,* in G. LATTANZI (a cura di), *Reati e responsabilità degli enti*, cit., 153 ss.

C. PIERGALLINI, *Paradigmatica dell'autocontrollo penale, Parte I e Parte II.*

C. PIERGALLINI, *Una sentenza "modello" della Cassazione pone fine all'estenuante vicenda "Impregilo",* in *Sist. Pen.*, 27 giugno 2022.

C. PIERGALLINI, voce *Colpa (diritto penale)*, in *Enc. Dir. Annali*, X, 2017, 224 ss.

N. PISANI, *I requisiti di autonomia e indipendenza dell'Organismo di Vigilanza istituito ai sensi del d.lgs. 231/2001*, in *Resp. amm. soc. enti*, 2008, 1, 155 ss.

G. PITRUZZELLA, *Big data, competition and privacy: a look from the antitrust perspective, concorrenza e mercato*, 2016, 15-20.

F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, 2018, Torino.

C. PONGILUPPI, *Principio di precauzione e diritto penale: nihil novi sub sole?*, in *Dir. pen. cont*., 2009, 252 ss.

G. PRESTI, *What We Talk About When We Talk About Compliance*, in S. MANACORDA-F. CENTONZE (Eds.), *Corporate Compliance on a Global Scale. Legitimacy and Effectiveness*, Springer 2022, p. 25 ss.

D. PULITANÒ, *La responsabilità "da reato" degli enti nell'ordinamento italiano,* in AA: VV., *Responsabilità degli enti per i reati commessi nel loro interesse,* Supplemento al n. 6 di *Cass. Pen.* 2003, 28 ss.

D. PULITANÒ, *La responsabilità da reato degli enti: i criteri d'imputazione*, in *Riv. It. Dir. e proc. pen*., 2002, 419.

D. PULITANÒ, *Organizzazione dell'impresa e diritto penale del lavoro*, in *Riv. Giur. Lav*., 1985, 3 ss.

M. RASKIN, *The Law and Legality of Smart Contracts*, in *Georgetown Law & Tech Review*, 1, 311.

Relazione al d. lgs. 8 giugno 2001, n. 231, 3.4, in *Guida dir*., 2001, 36.

P. RESCIGNO, *voce Capacità giuridica*, in *Dig. Disc. Priv*. (sez. civ.), II, Torino, 1988, 218 ss.

S. RIONDATO, *Robot, talune indicazioni di diritto penale*, in P. MORO, C. SARRA (a cura di), *Tecnodiritto*; D. LIMA, *Could AI Agents be held criminally liable?,* cit., 688 ss.

R. RORDORF, *La normativa sui modelli di organizzazione dell'ente*, in *Cass. Pen*., 2003, 6S, 79 ss.

M. ROMANO, *La responsabilità amministrativa degli enti, società o associazioni: profili generali*, in *Riv. soc*. 2002, 398.

M. RONCO, E. MEZZETTI, *Diritto penale d'impresa*, Bologna, 2009, 69.

A. ROSSI, *I piani per la prevenzione della corruzione in ambito pubblico e i modelli 231 in ambito privato,* in *Dir. pen. e proc., Speciale corruzione,* 2013, 45.

T. ROTSCH, *Criminal Compliance – Begriff, Entwicklung und theoretische Grundlegung,* in ID. (Hrsg.), *Criminal Compliance – Handbuch,* Nomos, Baden-Baden, 2015, p. 41 ss.

M. RUBINO - F. VITOLLA - N. RAIMO, *Il processo di digitalizzazione aziendale e la digital transformation,* 2020, 56.

M. RUBINO – F. VITOLLA – A. GARZONI, *Cultura nazionale e livello di digitalizzazione delle imprese europee: evidenze empiriche in Identità, innovazione e impatto dell'aziendalismo italiano,* a cura di F. CULASSO, M. PIZZO, Università di Torino.

U. RUFFOLO, *Il problema della personalità elettronica,* in U. RUFFOLO (a cura di), *L'intelligenza artificiale – Il diritto, i diritti, l'etica*, Milano 2020, 217.

U. RUFFOLO, *Intelligenza artificiale, machine learning e responsabilità da algoritmo,* in *Giur. It.*, 7, 2019, 1689.

U. RUFFOLO, *Per i fondamenti di un diritto della robotica self-learning, dalla machinery produttiva all'auto driverless: verso una responsabilità dell'algoritmo?*, in U. RUFFOLO (a cura di), *Intelligenza artificiale e responsabilità,* Milano, 2017, 13 ss.

R. A RUGGIERO, *Non prosecution agreements e criminalità d'impresa negli U.S.A.: il paradosso del liberismo economico*, in *Dir. pen. cont.*, 12 ottobre 2015.

Y. RUI, *From Artificial Intelligence to Augmented Intelligence*, in *IEEE MultiMedia*, gennaio 2017, vol. 24, n. 1, p. 4 ss.

S. J. RUSSEL-P. NORVING, *Artificial Intelligence – A modern approach*, 2010, 1020 ss.

P. M. SABELLA, *Vendita di società "ready made" ed obblighi di verifica della clientela nella disciplina sulla prevenzione di riciclaggio e finanziamento del terrorismo: contrasto all'anonimato e valute virtuali. Nota a CGUE Grande sezione 17 gennaio 2018 (causa C.676/16)*, in *DPCE online*, 2018, 2, 545 ss.

R. SABIA, *Artificial Intelligence and Enviromental Criminal Compliance*, in *Revue Internationale de Droit Pènal*, 2020, 179-201.

R. SABIA, I. SLAVEMME, *Costi e funzioni dei modelli di organizzazione e gestione* ai sensi del d.lgs. n. 231/2001, in A. DEL VECCHIO, P. SEVERINO (a cura di), *Tutela degli investimenti tra integrazione dei mercati e concorrenza di ordinamenti*, Bari, 2016, 445 ss.

R. SABIA, *Responsabilità da reato degli enti e paradigmi di validazione dei modelli*, 2022, 99 ss.

G. SARTOR (eds), *AI Approaches to the Complexity of Legal Systems*, Berlin-Heidelberg, 2014, 153 ss.

G. SARTOR, *L'intelligenza artificiale e il diritto*, Torino, 2022.

A. SAVELYEV, *Contract law 2.0: Smart contracts as the beginning of the end of classic contract law, in information & Communications Technology Law*, 2017, 122 ss.

J. R. SEARLE, *"Minds, Brains and Programs"*, in *The Behavioural and Brain Science*, 1980, 417 ss.

N. SELVAGGI, *L'interesse dell'ente collettivo quale criterio di ascrizione della responsabilità da reato*, Jovene, 2006.

J. SEMYOR, P. TULLY, *Weaponizing Data Science for Social Engineering: Automated E2E Spear Phishing on Twitter*, 2016.

A. SERENI, *La colpa di organizzazione nella responsabilità dell'ente da reato. Profili generali*, in D. PIVA (a cura di), *La responsabilità degli enti ex d. lgs. n. 231/2001 tra diritto e processo*, 58 ss.

P. SEVERINO, *Il sistema di responsabilità degli enti ex d. lgs. 231/2001*, in F. CENTONZE – M. MANTOVANI (a cura di), *La responsabilità "penale" degli enti*, Bologna, 2016, 74.

P. SEVERINO, *La responsabilità dell'ente ex d.lgs. 231 del 2001: profili sanzionatori e logiche premiali*, Milano, 2018, 1122 ss.

P. SEVERINO, *Intelligenza artificiale e diritto penale*, Milano, 2020, 535 ss.

S. SHETTY - M. MUSA – X. BRÈDART, *Bankrupctcy prediction Using Machine Learning Techniques*, in *Journal of Risk and Financial Management*, 15, 35, 1-10.

G. J. SICIGNANO, *L'interesse e il vantaggio dell'ente nel riciclaggio mediante criptovalute,* in Riv. 231, 2021.

U. SIEBER, *The International Handbook on Computer Crime. Computer-related Economic Crime and the Infrigements of Privacy*, John Wiley Sons, New York, Brisbane, Toronto, Singapore, 1986.

M. SIMBULA, *La normativa italiana sulle DLT*, in *Blockchain e smart contract*, Milano, 2019, 135 ss.

A. SIMONCINI, S. SUWEIS, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto costituzionale*, in *Riv. fil. Dir*., 2019, 1, 93 ss.

P. STANZIONE, *Capacità e minore età nella problematica della persona umana*, Camerino-Napoli, 1975.

P. STANZIONE, *Capacità* (diritto privato), in *Enc. Giur.*, V, Roma, 1988, 6 ss.

F. STELLA, *Criminalità d'impresa: lotta di sumo e lotta di judo*, in *Riv. Trim. dir. pen. econ*., 2/3, 1998, 476.

F. STELLA, *Giustizia e modernità. La protezione dell'innocente e la tutela delle vittime,* Milano, 2003, 593 ss.

TCW LIN, *Compliance, technology, and modern finance*, in *Brooklyn Journal of Corporate, Financial and Commercial Law*, 2016, 11, 159-182.

C. THIBAULT, *Why your company needs a Chief Algorithms Officer*, 26 settembre 2018.

K. TIEDEMAN, *Die Bebußung von Unternehmen nach dem 2. Gesetz zur erkämpfung der Wirtshaftskriminalityt*, in *NJW*, 1988, 1169 ss.

U. TOMBRARI, *Intelligenza artificiale e corporate governance nella società quotata*, in *Dir. soc*., 2021, 1431.

P. TONINI, *Il valore probatorio dei documenti contenenti dichiarazioni scritte*, CP, 1990, 2219.

R. TREZZA, *I Valori giuridici possono mai trasformarsi in variabili algoritmiche? Brevi osservazioni su giurimetria, algo-crazia e algoretica*, in www.intelligenzaartificiale.unisal.it.

R. TREZZA, *L'intelligenza artificiale come ausilio alla standardizzazione del modello 231: vantaggi "possibili" e rischi "celati"*, in *Giurisprudenza Penale web*, 2021, 1-bis.

A. F. TRIPODI, *L'elusione fraudolenta nel sistema della responsabilità degli enti*, Padova, 2013.

A. F. TRIPODI, *Situazione organizzativa e colpa di organizzazione: alcune riflessioni sulle nuove specialità del diritto penale dell'economia*, in *Riv. Trim. dir. pen. ec.*, 2004, 483 ss.

A. F. TRIPODI, *L'elusione fraudolenta del modello. Ruolo e gestione ermeneutica del controverso inciso a venti anni dalla sua comparsa*, in D. PIVA (a cura di), *La responsabilità degli enti ex d. lgs. 231/2001 tra diritto e processo*, 230 ss.

A. M. TURING, *Computing Machinery and Intelligence*, in *Mind*, LIX, 1950, 433 ss.

D. C. VALADECK, *Machine without principals: liability rules and Artificial*, in *Washington Law Review*, 2014, 89, 150.

V. VALENTINI, *Colpa di organizzazione e misure di compliance*, in C. FIORIO (cur.), *La prova nel processo degli enti*, Torino, 2016, 82.

A. S. VALENZANO, *L'illecito dell'ente da reato per omessa o insufficiente vigilanza. Tra modelli preventivi e omesso impedimento del reato*, Napoli, 2019.

G. VARRASO, *Il procedimento per gli illeciti amministrativi dipendenti da reato*, in UBERTIS-VOENA, *Trattato di procedura penale*, Milano 2012, XLVII, 92.

P. VENTURA, *Le indagini difensive*, in UBERTIS-VOENA, *Trattato di procedura penale*, Milano, 2005, XXVII, 2, 124.

P. C. VERHOEF – T. BRORKHUIZEN – Y. BART – A. BHATTACHARYA – J. Q. DONG – N. FABIAN – M. HAENLEIN, *Digital transformation: A multidisciplinary reflection and research agenda*, in *Journal of Business Research*, 2019, 1-13.

E. VILLANI, *Alle radici del concetto di colpa di organizzazione nell'illecito dell'ente da reato*, Napoli, 2016, 80 ss.

L. VIZZONI, *Domotica e diritto. La Smart Home tra regole e responsabilità*, Milano, 2021, 35-36.

T. VITARELLI, *Delega di funzioni e responsabilità penale*, Milano, 2006.

K. WALCH, *Is there a Difference between Assisted Intelligence vs. Augmented Intelligence?*, in *Forbes*, 12 gennaio 2020.

G. WESTERMAN - C. CALMÈJANE – D. BONNET – P. FERRARIS – A. MCAFEE, *Digital transformation: a road-map for a billion-dollar organizations, MIT Center for Digital Business and Capgemini Consulting*, Cambdrige, 2011.

J. ZERILLI, A. KNOTT, J. MACLAURIN, C. GAVAGHAN, *Algoritmic Decision-Making and the Control Problem*, in *Minds and Machines*, 2019, 29, 555 ss.

C. ZOTT – R. AMIT, *Business Model Innovation – How to create Value in a Digita*l *World*, in *GfK Marketing Intelligence Review*, vol. 9, n. 1, 2017, 18-23.