RIFLESSI DELLA *COMPLIANCE* DIGITALE IN AMBITO 231 (*)

di Attilio Nisco

SOMMARIO: 1. Premessa: *compliance* digitale e intelligenza artificiale. – 2. Un triplice ordine di (possibili) ricadute. – 3. *Digital Criminal Compliance*, tra aspettative e rischi. – 4. Verso una ridefinizione dei compiti organizzativi degli amministratori. – 5. Riflessi sulla colpa d'organizzazione.

1. Premessa: *compliance* digitale e intelligenza artificiale.

L'espressione "*compliance* digitale" abbina due termini *à la page* nel dibattito giuridico contemporaneo (non solo penalistico). Nel contesto del presente contributo, l'espressione mira a focalizzare un ambito tematico di crescente impatto pratico e, crediamo, anche teorico: gli effetti dell'applicazione di tecnologie emergenti ai sistemi di *compliance* e, tra questi, ai modelli di organizzazione e gestione previsti dal d.lgs. 231/2001 (di seguito: MOG).

Ai fini di un corretto inquadramento della tematica, si richiedono alcune precisazioni.

La prima discende dalla pluridimensionalità del fenomeno "compliance". L'espressione compendia un «vasto e composito universo»[1] di misure organizzative di contenimento del rischio "di non conformità" (e dunque di incorrere nelle conseguenti sanzioni), rilevante a più livelli: aziendale, legale e più specificatamente penale (*criminal compliance*)[2]. Data la varietà dei fini, la *compliance* si connota più per i mezzi impiegati – costituiti, in sintesi, da protocolli organizzativi e sistemi di analisi e controllo dei rischi –, che per uno specifico obiettivo.

Ne segue che il fenomeno della digitalizzazione non riguarda solo l'attuazione di tecnologie informatiche dirette a minimizzare il rischio reato; interessa, più in generale, gli adempimenti organizzativi vigenti in ambito corporativo (coinvolgenti l'analisi dei rischi e le strutture di *corporate governance*), come pure l'ordinario svolgimento di vari processi aziendali interni (si pensi alla fissazione di premi di retribuzione o dei prezzi di vendita di un prodotto) ed esterni (con particolare

(*) Contributo destinato al volume "*La responsabilità da reato degli enti: profili dogmatici e politico-criminali*", a cura di L. CORNACCHIA – E.D. CRESPO, editore Giappichelli.

[1] V. MONGILLO, *Presente e futuro della compliance penale*, in *Sist. pen.*, 11 gennaio 2022, p. 1.

[2] Delucidazioni sul concetto di "compliance", muovendo dalla sua ambiguità, in 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.; con più specifico riferimento alla "compliance penale", T. ROTSCH, *Criminal Compliance – Begriff, Entwicklung und theoretische Grundlegung*, in ID. (Hrsg.), *Criminal Compliance – Handbuch*, Nomos, Baden-Baden, 2015, p. 41 ss.

Editore Associazione "Progetto giustizia penale" | via Festa del Perdono 7, 20122 Milano
c/o Università degli Studi di Milano, Dipartimento di Scienze Giuridiche "Cesare Beccaria"
redazione@sistemapenale.it

riferimento ai travolgenti sviluppi del *trading* finanziario). D'altro canto, sempre più spesso si parla di "*compliance* integrata", con riferimento tanto al coordinamento tra misure organizzative previste da varie fonti normative, quanto all'utilizzo di strumenti tecnologici per la gestione integrata di tali misure[3].

La prassi internazionale ha coniato etichette certamente evocative di una gestione integrata dei processi: l'acronimo "GRC" (*governance*, *risk management and compliance*) esprime l'interdipendenza tra processi decisionali (*governance*), di valutazione preventiva dei rischi (*risk management*) e di adozione di condotte *lato sensu* "conformi" (*compliance*)[4]. Per quanto tali strumenti operino su piani distinti e richiedano gradi diversificati di implementazione, a seconda del tipo di impresa e/o di attività, nessuno di questi piani può essere preventivamente ignorato nell'impostare un'analisi del fenomeno e, di conseguenza, dell'impatto su di esso della digitalizzazione.

Nella prospettiva del diritto italiano, sintomo evidente della trasversalità del concetto di *compliance* è il nesso normativo che viene instaurandosi tra MOG e diritto societario, osservabile nella progressiva affermazione di obblighi organizzativi a carico dei vertici dell'impresa societaria, culminata nella riformulazione dell'art. 2086 c.c.[5].

Una seconda precisazione attiene al tipo di tecnologia cui nel prosieguo faremo riferimento; dunque, all'aggettivo "digitale". Evidente che con esso si richiami il passaggio dall'analogico al digitale, ossia la "digitalizzazione" che ha interessato – tra le altre cose – l'organizzazione aziendale, da ultimo nelle forme della c.d. "Industria 4.0". Quando si parla di "*compliance* digitale", si pensa anzitutto alla gestione dei dati, al rispetto della normativa sulla riservatezza e alla prevenzione degli illeciti (compresi alcuni reati informatici) che possono derivarne[6]. In tale prima accezione, il rapporto tra *compliance* e digitalizzazione risulta ambivalente: da un lato, esso guarda alla prevenzione delle violazioni di cui si è appena detto, costituendo un ulteriore ambito della *compliance* generale; dall'altro lato, proprio questa *compliance* in materia di riservatezza rappresenta un limite generale alle misure di *compliance* attuate (e attuabili) in altri settori, per l'ovvia ragione che – almeno di regola – la corretta applicazione della normativa sulla riservatezza è un presupposto per la valida implementazione di un sistema di *compliance*[7].

In questa sede, però, l'espressione "*compliance* digitale" sarà riferita all'impiego, in ambito aziendale, di tecnologie basate sull'Intelligenza Artificiale (di seguito: IA) e, in

---

[3] A. GULLO, *I modelli organizzativi*, in G. LATTANZI-P. SEVERINO (a cura di), *Responsabilità da reato degli enti*, vol. I., Giappichelli, Torino, 2020, p. 284 ss.

[4] Cfr. G.P. MILLER, *The Law of Governance, Risk Management and Compliance*, 2nd ed., Wolters Kluwer, New York, 2017, p. 1 ss. Nel dibattito tedesco, sulla necessità di coordinamento del *Compliance Mangement System* con il GRC, S. GRÜNINGER, *Grundlagen einer wertorientierten Compliance*, in J. WIELAND-R. STEINMEYER-S. GRÜNINGER (Hrsg.) *Handbuch Compliance-Management. Konzeptionelle Grundlagen, praktische Erfolgsfaktoren, globale Herausforderungen*, 3. Aufl., E. Schmidt Verlag, Berlin, 2020, p. 57.

[5] Sul punto v. anche V. MONGILLO, *Presente e futuro*, cit., p. 5.

[6] Cfr. A. GESCHONNECK, *Cyber- und Privacy Compliance*, in *Handbuch Compliance-Management*, cit., p. 1067 ss.

[7] Cfr. J. EISELE, *Datenschutzstrafrecht*, in *Criminal Compliance*, cit., pp. 764-765, il quale evidenzia anche il potenziale conflitto tra queste due prospettive.

particolare, alla IA applicata ai *Big Data*[8]. È questa la forma di tecnologia, connessa all'universo digitale, che desta maggiore interesse sul piano delle implicazioni sociali[9]. Diviene però necessario ovviare a una difficoltà definitoria. È risaputo come l'IA non sottostia a nessuna definizione condivisa, di tipo scientifico, sociologico e tanto meno normativo, e nondimeno susciti gli sforzi definitori di varie "agenzie" attive nel campo delle politiche pubbliche[10]. Possiamo quindi assumere come punto di riferimento la definizione contenuta all'art. 3 della "Proposta di regolamento europeo" del 21 aprile 2021, secondo la quale la caratteristica dell'IA è «un *software* sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I [allo stesso regolamento, nda], 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»[11].

Premesso che la componente umana non è, almeno al momento, eliminabile, e che dunque si richiede una necessaria interazione tra macchina e uomo, le varie applicazioni dell'IA denotano semmai un livello differenziato di emancipazione della macchina dall'uomo. Tuttavia, l'aspetto più innovativo della tecnologia in questione, evidenziato anche dalla definizione sopra citata, è la sua capacità di autodeterminarsi, cioè di orientare l'analisi autonomamente, elaborando una mole enorme di dati in tempi estremamente ridotti (cosa che nessun uomo riuscirebbe a fare) e, soprattutto, senza limitarsi a riprodurre schemi decisionali preimpostati, bensì adottando scelte operative che non richiedono l'intervento umano[12], come sono capaci di fare gli algoritmi "intelligenti".

2. Un triplice ordine di (possibili) ricadute.

Proprio in ragione di questo suo connotato, che va oltre la semplice automazione, l'impiego delle tecnologie alle quali si è da ultimo accennato suscita, in via generale, problemi di allocazione della responsabilità, tanto da dare adito ad ardite proposte di

---

[8] In questi termini, C. BURCHARD, *Digital Criminal Compliance*, in *Festschrift für U. Sieber zum 70. Geburtstag*, II, Duncker & Humblot, Berlin, 2021, p. 742 ss. Nella medesima prospettiva, P.A. RAMIREZ BARBOSA, *Corporate Criminal Law, Artificial Intelligence and Big Data: the Huawei Case and its Implications for Global Society*, in *Revista Paradigma*, v. 29, n. 1, 2020, p. 19 ss. (*https://revistas.unaerp.br/*).

[9] A. ELLIOTT, *La cultura dell'intelligenza artificiale. Vita quotidiana e rivoluzione digitale* (trad. it., di *The Culture of AI. Everyday Life and the Digital Revolution*, 2019), Codice Edizioni, Torino, 2021.

[10] Cfr. A. ELLIOTT, *La cultura dell'intelligenza artificiale*, cit., p. 26.

[11] Commissione europea, *Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione*, 21 aprile 2021, in *https://eur-lex.europa.eu*. Per un'introduzione, A. LAVORGNA-G. SUFFIA, *La nuova proposta europea per regolamentare i Sistemi di Intelligenza Artificiale e la sua rilevanza nell'ambito della giustizia penale*, in *Dir. pen. cont. – Riv. trim.*, 2/2021, p. 88 ss.

[12] Questo aspetto è comunemente segnalato dalla letteratura specialistica (non solo giuridica); per limitarci ai penalisti, v. L. PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in AA.VV., *Cybercrime*, Utet-Wolter Kluwers, Milano, 2019, p. 45.

estendere la responsabilità penale alle macchine[13]. Questo tema interseca la responsabilità degli enti a più livelli, vuoi perché la responsabilità degli enti si basa a sua volta su una *fictio*, che si potrebbe – invero impropriamente[14] – trasporre alla macchina, vuoi perché, quand'anche si respingesse – come ritengono in molti – un'autonoma soggettività dell'IA, la sostituzione di operatori umani con algoritmi porrebbe comunque una questione di imputazione all'ente di eventi prodotti dal cattivo funzionamento delle macchine[15].

In questa sede, ci asterremo anche solo dallo sfiorare il tema di un'avveniristica soggettività giuridica (e giuridico penale) della macchina, come pure di un suo improbabile parallelo con quella dell'ente, provando invece a riflettere sui potenziali effetti dell'IA nella distribuzione delle responsabilità tra uomo ed ente e all'interno dell'ente. Se assumiamo, nel nostro ordinamento, il sistema delineato dal d.lgs. 231/2001 come centrale, anche se non esaustivo, del concetto di "compliance" (secondo le precisazioni formulate *supra*, § 1), possono essere individuati almeno tre livelli di interferenza tra tecnologie basate sull'IA e responsabilità di individui ed enti.

In primo luogo, tali tecnologie hanno un impatto (e sono destinate ad averlo in misura crescente) sulle modalità operative relative al controllo e alla prevenzione dei reati in ambito aziendale, integrando o sostituendo le misure organizzative ordinariamente impiegate a tale scopo. In tale prospettiva, la tecnologia incide sulla "*compliance* penale" in senso stretto, delineando un'area che la dottrina ha inquadrato in termini di *Digital Criminal Compliance* [16] (*infra*, § 3).

In secondo luogo, la tecnologia basata sull'IA incide sulla definizione e sulla distribuzione dei compiti organizzativi spettanti al *management* della società, a cominciare dagli amministratori. Da quest'angolo visuale, che potremmo denominare di *Corporate Technology*[17], l'IA potrebbe avere effetti sui consueti criteri di imputazione della responsabilità (anche) penale dei vertici e dei controllori aziendali (§ 4).

Infine, con più specifico riferimento alla responsabilità dell'ente, le nuove tecnologie potrebbero mutare sensibilmente il nostro modo di concepire e di applicare la c.d. colpa di organizzazione e, con essa, la responsabilità penale o para-penale degli enti[18] (§ 5).

---

[13] Per un esame critico di tali proposte, A. CAPPELLINI, Machina delinquere non potest? *Brevi appunti su intelligenza artificiale e responsabilità penale*, in *disCrimen*, 27 marzo 2019; C. PIERGALLINI, *Intelligenza artificiale: da "mezzo" a "autore" del reato?*, in *Riv. it. dir. proc. pen.*, 2020, p. 1745 ss.

[14] P. SEVERINO, *Intelligenza artificiale e diritto penale*, in U. RUFFOLO (a cura di), *Intelligenza artificiale – Il diritto, i diritti, l'etica*, Giuffrè, Milano, 2020, p. 535.

[15] Cfr. M.E. DIAMANTIS, *The Extended Corporate Mind: When Corporations Use AI to Break the Law*, in *North Carolina Law Review*, 98(4), 2020, p. 898 ss.

[16] C. BURCHARD, *Digital Criminal Compliance*, cit.

[17] Cfr. L. ENRIQUES, *Responsabilità degli amministratori e ruolo degli algoritmi: brevi annotazioni sul senno di poi 4.0*, in *Intelligenza artificiale – Il diritto, i diritti, l'etica*, cit., p. 295 ss.

[18] Sul tema, ovviamente, pesa anche il diverso modo di concepire la responsabilità degli enti; da diverse angolature, v. M.E. DIAMANTIS, *The Extended Corporate Mind*, cit., p. 893 ss.; FED. MAZZACUVA, *The Impact of AI on Corporate Criminal Liability: Algorithmic Misconduct in the Prism of Derivative and Olistic Theories*, in *Revue Internationale de Droit Pénal*, Vol. 92, 1, 2021, p. 143 ss.; N. SELVAGGI, *Dimensione tecnologica e* compliance *penale: un'introduzione*, in L. LUPÀRIA-L. MARAFIOTI-G. PAOLOZZI (a cura di), *Dimensione tecnologica e prova*

3. *Digital Criminal Compliance*, tra aspettative e rischi.

La *Digital Criminal Compliance* si insinua nelle maglie di una più vasta offerta di servizi di gestione digitale della *compliance tout court* presenti sul mercato. Il che è del resto in linea col fatto che la *compliance* penale, più che come autonomo fenomeno normativo, si atteggia a derivato di un più generale cambiamento prodotto, nella realtà delle imprese, dalla prassi della *compliance*[19]. Per quanto non sia sempre facile cogliere, sul piano strettamente tecnologico, come operino i nuovi strumenti, né sia agevole discernere gli sviluppi futuri da quelli già in atto, emerge chiaramente quale sia l'apporto innovativo delle nuove tecnologie: esse consentono di individuare (o quantomeno ambiscono a farlo) tempestivamente delle irregolarità, sì da dotare "finalmente" di una reale efficacia preventiva l'azione della *compliance*. «Gli algoritmi – si è scritto – forniscono i dati rilevanti in "tempo reale", con una costante prontezza operativa, in una griglia temporale predefinita per un determinato risultato di elaborazione. Essi spezzano una delle principali debolezze dei modelli di *compliance* convenzionali: essendo questi ultimi basati solo su dati storici, raramente residua la possibilità operativa di prevenire una violazione delle regole […]. Le analisi in tempo reale, per contro, permettono di seguire le strutture comportamentali nel loro processo di sviluppo e di distinguere qualitativamente se e quando le regole saranno probabilmente ignorate o alla fine rispettate. Da ciò si riduce la percentuale di sospetti infondati, mentre l'efficienza dei sistemi di *compliance* aumenta in modo sostanziale»[20].

Quanto alle possibili applicazioni nella prevenzione del rischio reato, che spaziano tra contesti molto vari («dal furto di *routine* dei dipendenti all'*insider trading*»)[21], occorre osservare che, in alcuni casi, la digitalizzazione pervade la struttura stessa dell'attività, di base lecita, sulla quale questo rischio si innesta. È il caso, oltre che dei reati informatici (realizzabili sovente a danno della stessa impresa, tenuta ad integrare il proprio sistema di *compliance* con specifiche misure di sicurezza), soprattutto degli abusi di mercato (manipolazione e *insider trading*). La finanza tecnologica è difatti il settore trainante della digitalizzazione della *compliance*[22], essendo gli scambi borsistici regolati

---

penale, Giappichelli, Torino, 2019, p. 217 ss.

[19] Sul rapporto tra *compliance* in generale e *compliance* penale, in questi termini, T. ROTSCH, *Criminal Compliance*, cit., p. 41.

[20] S. NEUFANG, *Digital Compliance – Wie digitale Technologien Compliance-Verstöße vorhersehen*, in *IRZ - Zeitschrift für Internationale Rechnungslegung*, 2017, p. 249. Una descrizione delle modalità operative della *compliance* digitale, di cui caldeggia l'utilizzo, anche in A. SCHEMMEL, *"Effective Corporate Governance" by Legal Tech/Digital Compliance*, in S. BREIDENBACH-F. GLATZ (Hrsg.), *Handbuch Legal Tech*, 2. Aufl., C.H. Beck, München, 2021, p. 166 ss. Invece, per un approccio critico all'automazione informatica della *compliance*, già K.A. BAMBERGER, *Technologies of Compliance: Risk and Regulation in Digital Age*, in *Texas Law Rev.*, 88, 4, 2010, p. 669 ss.

[21] L. QUEST, A. CHARRIE, L. DU CROO DE JONGH S. ROY, *The Risks and Benefits of Using AI to Detect Crime*, in *Harvard Business Review* (https://hbr.org/), August 9, 2018.

[22] Sul punto, M. MOZZARELLI, *Digital Compliance: The Case for Algorithmic Transparency*, in *Corporate Compliance on a Global Scale*, cit., p. 259 ss.

da un sistema automatizzato di transazioni (*High Frequency Trading*), che ne garantisce la massima celerità ed economicità. Innestandosi in un sistema di tal fatta, la stessa condotta criminale di abuso del mercato risulta dematerializzata[23]. La digitalizzazione della *compliance* diviene allora un riflesso condizionato di questa evoluzione: la misura preventiva è chiamata ad adeguarsi al tasso tecnologico della condotta criminale[24]. Ma l'impiego di IA, in questi casi, pone anzitutto un problema di dispersione della responsabilità: essendo la condotta realizzata tramite strumenti tecnologici, la responsabilità potrebbe risalire al programmatore, installatore etc.; ed infine all'ente (magari attraverso l'art. 8 del decreto 231)[25], reo di non aver presieduto a questi processi o di non aver predisposto le adeguate contromisure tecnologiche.

Per certi versi correlati a tali aspetti sono gli sviluppi in atto nel settore dell'antiriciclaggio, dove la verifica delle operazioni sospette e la verifica della clientela saranno affidate in modo crescente a strumenti di IA, biometrici e di *Blockchain*[26]. Anche qui, la condotta può subire quel processo di dematerializzazione già indicato, per esempio nel caso in cui la condotta di riciclaggio o reimpiego passi attraverso l'operatività con criptovalute[27].

Ma la frontiera della *compliance* digitale non si arresta certo ai rischi connaturati ad un tessuto – per così dire – tecnologico di base. Nel settore ambientale, ad esempio, si prospetta l'impiego di *software* in grado di monitorare il superamento dei limiti soglia concernenti le condotte inquinanti[28]. Ed analoghe risorse tecnologiche potrebbero essere messe al servizio del *Tax Compliance System*, sino a pervenire all'automatica compilazione di dichiarazioni fiscali aziendali prive di infrazioni[29].

Inoltre, le nuove tecnologie potrebbero presto assolvere la funzione precipua di controllare il comportamento umano dal quale origina la commissione di qualsiasi reato. È quanto ci si attende, ad esempio, dall'impiego dell'IA nella prevenzione della corruzione[30], attraverso strumenti che consentirebbero di ricavare, in modo tempestivo e costante, segnali di allerta dallo scrutinio automatizzato di dati a disposizione

---

[23] F. CONSULICH, *Il nastro di Möbius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso di mercato*, in *Banca, borsa tit. cred.*, 2018, p. 195 ss.

[24] Cfr. J. BRÜNING, *Künstliche Intelligenz und strafrechtliche Haftung – Compliance-Anforderungen im digitalen Zeitalter mit Blick auf die Finanzwirtschaft*, in T. ROTSCH (Hrsg.), *Criminal Compliance – Status quo und Status futurus*, Nomos, Baden-Baden, 2021, p. 63 ss., spec. p. 76 ss.

[25] V. le riflessioni di F. CONSULICH, *Il nastro di Möbius,* cit., p. 228 ss.

[26] A. PERRONE, *La nuova vigilanza.* Regtech *e capitale umano*, in *Banca, borsa tit. cred.*, 2020, pp. 518-519.

[27] Entità che la giurisprudenza ha finito con l'assimilare, sia pure discutibilmente, alla nozione di prodotto finanziario ai fini dell'applicazione della fattispecie di abusivismo finanziario (art. 166 TUF): Cass., sez. II pen., 17 settembre 2020, n. 26807, in *Sist. pen.*, con commento di F. DALAITI, *Criptovalute e abusivismo finanziario: cripto-analogia o interpretazione estensiva*, *ivi*, 21 gennaio 2021.

[28] R. SABIA, *Artificial Intelligence and Environmental Criminal Compliance*, in *Revue Internationale de Droit Pénal,* 2020, p. 179 ss.

[29] Cfr. W. NIEMANN, *Aufbau und digitale Umsetzung eines Tax Compliance Management Systems*, in *DStR* (*Deutsches Steuerrecht*), 2021, p. 392 ss.

[30] Diffusamente, L. BIRRITTERI, Big Data Analytics *e* compliance *anticorruzione. Profili problematici delle attuali prassi applicative e scenari futuri*, in *Dir. pen. cont. – Riv. trim.*, 2/2019, p. 289 ss.

dell'organizzazione (movimenti anomali di risorse finanziare, anomalie nella fissazione dei prezzi etc.) o acquisiti da fonti esterne (processando dati accessibili in rete).

Non è possibile, però, limitare l'impiego delle nuove tecnologie a una valutazione di dati su di un piano strettamente oggettivo (come nel caso del superamento di un valore soglia) [31], potendosi il dato atteggiare, da solo o in combinazione con altri fattori, a indice sintomatico di un possibile comportamento deviante. Questa potenzialità applicativa suscita maggiori perplessità.

Certamente, infatti, in tutti gli esempi fatti in precedenza (ed altri ancora se ne potrebbero fare)[32], la tecnologia può contribuire a migliorare la gestione dei rischi, limitando gli errori, accelerando i tempi e riducendo i costi, o finanche presentandosi come indispensabile segmento di una vigilanza finanziaria reimpostata su base tecnologica. Ma essa presenta anche non trascurabili pericoli, là dove, per l'appunto, dalla valutazione di dati oggettivi si passi alla predizione di comportamenti soggettivi. La tendenza comune – o la speranza di alcuni – di affidare all'IA la valutazione complessiva dei rischi di violazione di norme, e la prescrizione delle misure per fronteggiarlo, potrebbe difatti portare ad una predizione di comportamenti devianti sfociante in una sorta di "prognosi di pericolosità" per singoli o per classi di individui attualmente o potenzialmente impiegati in un'organizzazione (o anche di altri soggetti destinatari del modello: consulenti, fornitori, partner, clienti etc.)[33].

Insomma: una profilazione di attitudini criminali di massa, che determinerebbe una trasposizione delle inquietudini suscitate alla polizia predittiva in contesti organizzativi (anche) privati.

Il primo argine a questo possibile sviluppo è costituito dalla normativa in materia di riservatezza. Va ricordato, a tal riguardo, che l'22 GDRP prevede un diritto alla trasparenza e alla "spiegazione" delle decisioni automatiche; per quanto gli esatti contorni di questa garanzia restino in parte incerti[34], è rilevante il fatto che essi si estendano alle decisioni adottate in un contesto privato, quale è l'impresa che adotti un sistema automatizzato di prevenzione dei reati. Inoltre, è chiaro che gli adempimenti relativi alla *compliance* non possono scriminare eventuali delitti a tutela della riservatezza informatica e della segretezza della corrispondenza. Dal punto di vista del diritto domestico, un ruolo peculiare riveste anche l'art. 4 dello Statuto lavoratori (l. 300/1970) che, in combinazione con l'art. 171 del *Codice privacy* (d.lgs. 196/2003), punisce già solo l'installazione di strumenti di controllo non autorizzati: sembra chiaro che l'impiego di una tecnologia per finalità di *compliance* debba comunque passare attraverso un'autorizzazione. Per effetto di riforme innescate dal c.d. *Jobs Act*, però, l'autorizzazione non è necessaria, se lo strumento di controllo coincide con uno

---

[31] Sulla sostanziale mancanza di criticità di valutazioni "oggettive", P. SEVERINO, *Intelligenza artificiale,* cit., p. 539.

[32] Cfr. L. QUEST-A. CHARRIE-L. DU CROO DE JONGH-S. ROY, *The Risks and Benefits*, cit.

[33] Approfonditamente, C. BURCHARD, *Digital Criminal Compliance*, cit., p. 747-748; al rischio di "algoritmi inquisitori" accenna anche N. SELVAGGI, *Dimensione tecnologica,* cit., p. 222.

[34] Sui complessi problemi definitori alla base dell'art. 22 GDPR, M. PALMIRANI, Big Data *e conoscenza*, in *Riv. filos. dir*., 1/2020, p. 73 ss.

"strumento di lavoro": nozione, quest'ultima, estremamente problematica, che rende dunque incerto il perimetro della tutela assicurata al dipendente[35].

Tutto ciò, però, ancora non basta a una piena tutela delle posizioni individuali colpite da decisioni automatizzate. Non a caso, la Proposta di regolamento europeo in materia di IA lascia supporre che l'utilizzo di questi sistemi rientrerà nella categoria dei sistemi di IA ad alto rischio, per l'impatto che essi potrebbero avere sul futuro delle persone controllate e dunque sui loro diritti fondamentali[36].

Infine, dietro lo sviluppo della *compliance* tecnologica si cela un'altra questione, spiccatamente penalistica. Gli strumenti tecnologici possono servire anche – se non soprattutto – nell'attività di indagine interna; di conseguenza, il loro uso acuisce la tensione tra diritto di difesa dell'ente e diritti degli individui coinvolti. La violazione delle norme in materia di riservatezza, allo stato, non impedisce l'acquisizione di materiale probatorio nel procedimento penale, attraverso il ricorso alla controversa figura dei "controlli difensivi"[37]. Viene in rilievo il tema della protezione dei dipendenti dalle auto-incriminazioni: profilo connesso alle indagini interne all'ente, e che rischia di essere, se non superato, certamente affiancato da quello della precostituzione di prove digitali (acquisibili come documenti), frutto sempre di indagini interne, resa notevolmente più agevole dalle nuove tecnologie. Anche per questo motivo pare necessaria una disciplina *ad hoc* delle indagini interne[38], che tenga conto delle nuove tecnologie impiegabili in questa fase e dell'utilizzabilità dei risultati in ragione di tutti gli interessi in gioco.

4. Verso una ridefinizione dei compiti organizzativi degli amministratori.

Dobbiamo adesso ampliare lo sguardo all'ingresso dell'IA nei consigli di amministrazione, per valutarne i potenziali effetti sulla distribuzione dei compiti e delle responsabilità tra i membri del consiglio, in generale e con specifico riferimento all'attuazione di un sistema di *compliance*, che rientra tra gli adempimenti organizzativi degli amministratori. Anche in questo caso è esclusa una totale automatizzazione dei processi decisionali interni al CdA; piuttosto, «la prospettiva più corretta è quella di vedere nell'IA non un sostituto, ma un sostegno degli amministratori, un sostegno nondimeno abile di per sé e non meramente servente»[39].

La tecnologia potrebbe aiutare gli amministratori nell'adempiere ai loro obblighi informativi o, più in generale, nell'attuazione di processi di *governance* e sistemi di controllo, in modo tale che gli stessi amministratori possano dedicarsi a tempo pieno alle

---

[35] In argomento, sia consentito rinviare a A. NISCO, *Prospettive penalistiche del controllo a distanza sull'attività lavorativa nell'attuale contesto normativo e tecnologico*, in *Sist. pen.*, 20 dicembre 2021.

[36] Cfr. Commissione europea, *Proposta di regolamento,* cit., considerando n. 36.

[37] V., ad es., Cass., sez. III pen., 14 dicembre 2020, n. 3255, in *DeJure*.

[38] Sul tema, v. E.M. MANCUSO, *"Indagini interne" disposte dall'ente: sussidiarietà regolatoria e nuovi scenari cooperativi*, in *Proc. pen. giust.*, 5/2020, p. 1254 ss.

[39] G.D. MOSCO, Roboboard. *L'Intelligenza artificiale nei consigli di amministrazione*, in *An. giur. ec.*, 1/2019, p. 249.

scelte imprenditoriali, cioè alla gestione. In sintesi, l'IA parrebbe poter sollevare gli amministratori dai compiti di *compliance*[40].

Al tempo stesso, però, nei consigli potrebbe essere incentivata la presenza di amministratori dotati di competenze tecniche specifiche. A ciò, per altro, le società potrebbero essere indotte dalle autorità di vigilanza di quei settori che, come il mercato finanziario, stanno subendo una pervasiva automatizzazione digitale. Per riflesso, anche il metodo seguito nei controlli interni dovrebbe subire un aggiornamento tecnologico[41].

Da ciò potrebbe derivare, innanzitutto, una rimodulazione della responsabilità degli amministratori: la diligenza, la correttezza e l'obbligo di agire informati andrebbero valutati anche alla luce delle conoscenze acquisibili tramite questi sistemi[42]. Con particolare riferimento all'obbligo di dotare la società di assetti organizzativi adeguati (art. 2086 c.c.), sorge la questione se l'algoritmo possa essere visto come un requisito da integrare necessariamente nell'organizzazione, o se comunque il ricorso a una tecnologia in grado di individuare tempestivamente dei segnali di allarme possa incidere sul corretto adempimento di tali obblighi organizzativi. La risposta che si tende attualmente a dare a un tale quesito è negativa[43]. Ma, nella misura in cui la *compliance* digitale prometta di conferire maggiore effettività ai presidi organizzativi, questa conclusione non può essere ritenuta definitiva.

Non appare dunque prematuro chiedersi se possano esserci riflessi sulla responsabilità penale degli amministratori**,** in particolare sulla responsabilità omissiva dei membri non esecutivi del CdA. Difatti, poiché il *software* "prescrive" azioni capaci di intervenire in tempo reale sulle fonti di rischio, la tecnologia pare accorciare la "distanza organizzativa" tra condotta omissiva e reato non impedito. Le possibili ripercussioni di tutto ciò sull'imputazione dell'evento non sono inimmaginabili: il sistema informatico potrebbe individuare l'azione doverosa, supponendone l'efficacia "impeditiva", e potrebbe favorire la percezione di segnali di allarme, o comunque suscitare, in eventuali inquirenti, l'impressione che tali segnali fossero evincibili da un suo corretto utilizzo. Si pensi, ad esempio, all'applicazione di tecnologie come *machine learning* e *deep learning* nella scoperta degli indici predittivi d'insolvenza[44] e alle ripercussioni che l'impiego di tali sistemi potrebbe avere, in futuro, nella ricostruzione delle responsabilità per omesso impedimento dei reati di bancarotta.

Deve invece escludersi che alla IA possa essere conferita una delega di funzioni, come pure che un sistema informatico possa essere nominato amministratore di società (al di là di qualche noto caso mediatico)[45], se non altro perché, non avendo il sistema

---

[40] G.D. MOSCO, Roboboard, cit., p. 253.

[41] A. PERRONE, *La nuova vigilanza,* cit., p. 516 ss.

[42] Cfr. L. ENRIQUES, *Responsabilità degli amministratori,* cit., p. 296 ss.

[43] In argomento, M.L. MONTAGNANI-M.L. PASSADOR, *Il consiglio di amministrazione nell'era dell'intelligenza artificiale: tra* corporate reporting, *composizione e responsabilità*, in *Riv. soc.*, 2021, p. 121 ss.

[44] Ne illustra i particolari tecnici S. BEGUM, *A Detailed Study for Bankruptcy Prediction by Machine Learning Technique*, in AA.VV., *Intelligent Suistainable Systems*, Springer, 2022, p. p. 201 ss.

[45] È il caso dell'algoritmo VITAL, nominato nel *board* di una società di Hong Kong, secondo notizie diffuse nel 2014; v. L.F. BISOZZI, *Deep Knowledge Ventures, un algoritmo scelto come membro del Cda,* in *www.huffingtonpost.it*, 14 maggio 2014.

capacità giuridica, non possono essergli attribuiti quei requisiti soggettivi di indipendenza, diligenza etc. riferibili agli amministratori[46]. In sostanza, non è ammissibile un "*roboboard*"[47], ma, secondo quanto esposto in precedenza, lo sviluppo dell'IA rende ipotizzabile la creazione di *board* di (umani) esperti di nuove tecnologie nell'ambito del CdA[48].

Sorge allora una questione più specificatamente attinente all'implementazione di un MOG: sarebbe possibile sostituire l'Organismo di vigilanza (previsto dall'art. 6 d.lgs. 231/2001) con un sistema informatico basato sull'IA? Invero, le ragioni che si oppongono alla creazione di un *roboboard* vietano l'istituzione di un "OdV algoritmico". Le stesse ragioni, però, non escludono affatto che l'OdV (composto da umani) possa, o addirittura debba, dotarsi di tecnologie in grado di individuare rischi di non conformità del MOG, nel modo più rapido ed efficace[49]. Come pure, non escludono che, nelle realtà di ridotte dimensioni, nelle quali il compito della vigilanza sul modello può essere assunto dagli stessi amministratori, questi ultimi debbano adempiervi sulla base dei più avanzati sistemi tecnologici.

5. Riflessi sulla colpa d'organizzazione.

Giungiamo, con ciò, a interrogarci sulle ripercussioni delle nuove tecnologie sul MOG. La premessa, desumibile da quanto detto sin qui, è che la pretesa di esattezza e di maggiore effettività, avanzata da queste tecnologie, è destinata a incidere sul formarsi di *best practices* e, dunque, sulla standardizzazione dei sistemi di *compliance*, quantomeno in alcuni settori. Il che potrebbe finire, progressivamente, col condizionare il giudizio di idoneità dei modelli organizzativi, che non adottano misure tecnologiche (ritenute non eludibili), o adottano sistemi (considerati) poco performanti. Senza contare il fatto che lo stesso accertamento tecnico relativo alla idoneità del modello potrebbe avvalersi della tecnologia informatica[50].

Ove ciò accadesse, il rimprovero all'ente potrebbe concentrarsi, in futuro, su un'idea di "agente modello collettivo" tecnologicamente avveduto. Non possono essere taciute alcune criticità insite in un simile scenario.

---

[46] G.D. MOSCO, Roboboard, cit., p. 256. Sui possibili impieghi dell'IA in ambito societario, v. anche N. ABRIANI, *La* corporate governance *nell'era dell'algoritmo. Prolegomeni a uno studio sull'impatto dell'intelligenza artificiale sulla* corporate governance, in *Nuovo dir. soc.*, 3/2020, p. 268 ss.; R.M. AGOSTINO, *Intelligenza artificiale e processi decisionali. La responsabilità degli amministratori di società*, in *Mercato concorrenza regole*, 2/2020, p. 371 ss.

[47] Il termine è preso da G.D. MOSCO, Roboboard, cit.

[48] Cfr. N. ABRIANI, *La* corporate governance, cit., p 272 ss.

[49] Una soluzione simile è stata prospettata da S. PREZIOSI, *Responsabilità da reato degli enti e intelligenza artificiale*, in *Resp. amm. soc. enti*, 4/2020, p. 173 ss., per il sistema di controllo di attuazione del modello organizzativo ai sensi dell'art. 30 d.lgs. 81/2008.

[50] Su tali aspetti si sofferma N. SELVAGGI, *Dimensione tecnologica,* cit., p. 223 ss., il quale intravede prospettive "dirompenti" per la responsabilità degli enti.

Anzitutto, è necessario ricordare che la "esattezza" delle scelte operative compiute dai sistemi di IA dipende da molte variabili (a cominciare dal tipo di dati elaborati) e non è esente da "pregiudizi" o *bias*, perché comunque l'algoritmo è impostato su avvenimenti del passato. Tra questi pregiudizi rientra anche il c.d. *automation bias*, cioè la convinzione che la soluzione elaborata dalla macchina sia per ciò solo l'unica corretta[51]. Questa convinzione può essere tanto più fuorviante, se si considera che il risultato atteso riguarda la prevenzione di un comportamento descritto da norme penali soggette a interpretazione e, in molti casi, formulate in modo poco chiaro, se non indeterminato.

Da un lato, dunque, occorre rammentare il problema – più generale – della falsa neutralità dei sistemi predittivi basati sull'IA, che attiene al fondamento epistemologico stesso della predizione algoritmica[52]. Dall'altro lato, sia pure in un contesto privato (qual è l'organizzazione aziendale), si ripropone il dubbio inerente alla compatibilità tra un sistema predittivo di tipo informatico e un comportamento contrario a una norma, da giudicare illecito (o comunque deviante) solo al termine di un procedimento logico di sussunzione entro una fattispecie, che la macchina può emulare – o anche aiutare ad impostare –, ma non risolvere compiutamente[53].

Inoltre, riduzione degli errori operativi non vuol dire infallibilità del sistema preventivo-predittivo. Possono palesarsi disfunzioni in fase di funzionamento dei presidi di controllo, come pure a monte in sede di analisi del rischio. In linea di principio, una volta immessa una determinata tecnologia nell'organizzazione, il suo fallimento concorre al difetto organizzativo, il quale, a sua volta, potrà risalire anche alla fase di progettazione del sistema informatico di gestione del rischio. In questo modo, però, la comprensione del difetto organizzativo non è più alla portata del singolo ente, che, di norma, si è affidato a operatori altamente specializzati.

Cosicché, da questo punto di vista, la *compliance* digitale è destinata ad incidere anche sulla logica della auto-normazione, che presiede al concetto di *compliance* e che caratterizza, in larga parte, anche il sistema 231, mettendo a rischio, con ciò, il fondamento stesso del giudizio di rimproverabilità nei confronti dell'ente[54]. L'elaborazione di una complessa metodologia di analisi organizzativa transiterebbe, nei fatti, a un gruppo di esperti, secondo una dinamica che meriterebbe un'autonoma regolazione. La materia andrebbe verosimilmente ricondotta alla categoria dei "sistemi di IA ad alto rischio" contenuta nella proposta di regolamento europeo a cui si è fatto cenno[55].

---

[51] Cfr. K.A. BAMBERGER, *Technologies of Compliance*, cit., p. 676.

[52] Evidentemente, il tema è gravido di numerose questioni politico sociali, rilevanti su vasta scala: tra le altre, v. la densa trattazione di T. NUMERICO, Big data *e algoritmi. Prospettive critiche*, Carocci, Roma, 2021.

[53] Spunti interessanti in D. TIMMERMANN-K. GELBRICH, *Können Algorithmen subsumieren? Möglichkeiten und Grenzen von Legal Tech*, in *NJW*, 2022, p. 25 ss., che giudicano possibile l'impiego di algoritmi nella decisione giudiziale solo alla luce di una semplificazione del metodo giuridico.

[54] Analoghi rilievi in P. SEVERINO, *Intelligenza artificiale,* cit., p. 538.

[55] Commissione europea, *Proposta di regolamento*, cit., art. 9 ss. (ove, per altro, si dedica una specifica attenzione agli enti creditizi: ivi, art. 9, co. 9).

Per preservare il paradigma di una responsabilità per fatto proprio dell'ente, imputabile per colpa d'organizzazione, si potrebbe anche ipotizzare un obbligo di includere degli esperti nel perimetro dell'organizzazione. Si tratterebbe, in sostanza, di elaborare una "*compliance* della *compliance*" digitale, assecondando un meccanismo tipico di moltiplicazione dei controlli segnalato dalla sociologia dei sistemi. Non è affatto detto, però, che gli esperti siano sempre in grado di fornire una spiegazione esaustiva del difetto organizzativo eventualmente occorso a causa – o nonostante – l'impiego della tecnologia. Come noto, uno dei principali problemi dell'IA è la trasparenza delle decisioni, la cui imprevedibilità è insita nella stessa creazione di tali sistemi: neanche il programmatore (o comunque il creatore) è in grado di prevedere compiutamente le "decisioni" della macchina; si è parlato, al riguardo, di una «imprevedibilità prevedibile»[56].

Con ciò, la *compliance* digitale diviene il crocevia tra la questione della ricostruzione di un'autentica colpa d'organizzazione e l'altra, altrettanto cruciale questione della impellente necessità di regolamentare l'IA.

Lo sbocco, piuttosto scontato, di queste considerazioni non può che essere un auspicio a ricomprendere nell'ambito tematico della *compliance* digitale anche l'esigenza di regolamentarne l'uso prospettabile nelle organizzazioni d'impresa, cercando di mantenere fermo, fin dove possibile, il modello della "auto-regolazione regolata" che, faticosamente, si è cercato di sviluppare per la responsabilità degli enti. Tenendo insomma avvinte "*governance* tecnologica" e "*governance* della tecnologia", di modo che non solo l'organizzazione d'impresa si avvalga delle nuove tecnologie, ma che anche la tecnologia possa avvalersi delle organizzazioni, ricevendone un assetto di regole condivise e condivisibili.

[56] C. PIERGALLINI, *Intelligenza artificiale*, cit., p. 1762.