RIVISTA DI

POLITICA ECONOMICA

VETTORE IA
ALGORITMI, IMPRESA, SOCIETÀ

INTRODUZIONE **STEFANO MANZOCCHI, PAOLO SPAGNOLETTI**

Alessandro Aresu
Federica Ceci
Simone Saverio Fildi
Francesco Filippucci
Giusella Finocchiaro
Maria Teresa Gonnella
Simone Guarino
Antonio Gullo
Giuseppe F. Italiano
Cecilia Jona-Lasinio
Luigi Laura
Filippo Marchesani
Giuseppe Nicoletti
Rossella Sabia
Roberto Setola
Paolo Spagnoletti
Tiziano Volpentesta

N. 2-2024

CONFINDUSTRIA

Rivista di
Politica Economica

Direttore: Stefano Manzocchi

RIVISTA DI
POLITICA ECONOMICA
VETTORE IA
ALGORITMI, IMPRESA, SOCIETÀ

Introduzione . . . . . pag. 5
Stefano Manzocchi, Paolo Spagnoletti

PARTE PRIMA
INTELLIGENZA ARTIFICIALE: NATURA, EVOLUZIONI, SCENARI

Intelligenza artificiale: sviluppi, opportunità e sfide . . . . . » 11
Giuseppe F. Italiano

Come apprendono le macchine? . . . . . » 31
Luigi Laura

Geopolitica dell'intelligenza artificiale . . . . . » 53
Alessandro Aresu

Regolare l'intelligenza artificiale . . . . . » 73
Giusella Finocchiaro

Intelligenza artificiale e produttività: quadro concettuale, prime evidenze e traiettorie future . . . . . » 87
Francesco Filippucci, Cecilia Jona-Lasinio, Giuseppe Nicoletti

PARTE SECONDA
L'IA E LE IMPRESE

Intelligenza artificiale generativa nelle piccole e medie imprese: evidenze empiriche nel contesto italiano . . . . . » 113
Paolo Spagnoletti, Tiziano Volpentesta

Il ruolo dell'intelligenza artificiale come strumento organizzativo e strategico nelle *smart city* . . . . . » 131
Filippo Marchesani, Federica Ceci

Intelligenza artificiale e *compliance* penale. Scenari attuali e prospettive evolutive . . . . . » 149
Antonio Gullo, Rossella Sabia

IA per la *cybersecurity* . . . . . » 173
Simone Saverio Fildi, Maria Teresa Gonnella, Simone Guarino, Roberto Setola

Intelligenza artificiale e *compliance* penale. Scenari attuali e prospettive evolutive

Antonio Gullo, Rossella Sabia*

• *Le nuove tecnologie rappresentano un orizzonte particolarmente promettente per la* compliance *aziendale, ivi incluso quel peculiare comparto volto alla prevenzione dei reati all'interno delle organizzazioni. Obiettivo del contributo è condurre una riflessione sullo stato dell'arte della* digital criminal compliance*, dapprima esaminando alcune applicazioni di interesse – quali l'IA per la* data analytics *e la tecnologia* blockchain *–, per poi procedere a una verifica dell'impatto di simili innovazioni sul delicato terreno della responsabilità da reato degli enti di cui al D.Lgs. n. 231/2001, da ultimo anche alla luce del Regolamento europeo sull'intelligenza artificiale. Nella parte conclusiva, si getta lo sguardo, in ottica comparata, alle recenti novità legate all'inclusione dei rischi tecnologici nelle linee guida sulla valutazione dei* compliance program *del Department of Justice statunitense.*

JEL Classification: K14, K24, K42.

Keywords: *digital criminal compliance*, responsabilità da reato degli enti, modelli organizzativi, D.Lgs. n. 231/2001, intelligenza artificiale, *AI Act.*

* agullo@luiss.it, Università Luiss Guido Carli; rsabia@luiss.it, Università Luiss Guido Carli. Il lavoro è frutto di riflessioni congiunte degli autori. In particolare, il paragrafo introduttivo e quello conclusivo sono da attribuire a entrambi; Antonio Gullo è autore del paragrafo 2 e Rossella Sabia è autrice del paragrafo 3.

1. Nuove tecnologie e *corporate criminal compliance*: un inquadramento

Il ricorso a nuove tecnologie, e più in particolare all'intelligenza artificiale, rappresenta oggi una preziosa risorsa anche per la realtà delle imprese, chiamate a conformarsi a obblighi legali negli ultimi decenni in costante aumento, per mole, intensità e complessità.

Non sorprende pertanto constatare che, se il contesto organizzativo di riferimento per l'impiego di tali *tool* era rappresentato, in origine, da soggetti operanti in settori altamente regolamentati, quali le istituzioni finanziarie, lo scenario attuale appaia profondamente mutato. La varietà e flessibilità delle soluzioni tecnologiche disponibili sul mercato ha ampliato la platea delle organizzazioni interessate alla digitalizzazione di segmenti di attività: si è registrato, per quanto qui di maggior rilievo, un notevole incremento nel periodo post pandemico in ambito *e-commerce*, *healthcare*, *cybersecurity* dell'adozione di applicativi riconducibili all'area della c.d. *RegTech*[1] – con la previsione di una ulteriore crescita nel prossimo futuro, superiore ai 200 miliardi di dollari a livello globale entro il 2028[2].

D'altronde, si è già evidenziato l'impatto di tali tecnologie in ambito *corporate*[3] per perseguire obiettivi di maggiore efficienza e rapidità nelle attività volte a garantire il rispetto della normativa e, in generale, di requisiti legali, standard e *policy* rilevanti – in una parola, per la *compliance* aziendale. In tale area, un ruolo chiave è stato tradizionalmente riservato al 'fattore umano', dal momento che larga parte delle analisi, delle verifiche e dei controlli sulla conformità legale richiedono elevata qualificazione e specializzazione professionale; ma proprio la *over-regulation* di cui si diceva, determinando l'esponenziale aumento

---

[1] La *RegTech*, dall'unione, come si sa, delle parole *regulation* e *technology*, si riferisce all'uso della tecnologia nel contesto del monitoraggio, del *reporting* e della *compliance* normativa. Nella definizione dell'Institute of International Finance, si tratta dell'impiego di nuove tecnologie per rispondere in modo più efficace alle richieste regolatorie e di conformità (IIF, "Regtech in Financial Services: Technology Solutions for Compliance and Reporting", 2016, p. 2, https://www.iif.com/portals/0/Files/content/RegTech%20in%20Financial%20Servies.pdf. Sulla *RegTech* per la *compliance* aziendale, cfr. Barberis J., Arner D.W., Buckley R.P. (a cura di), *The RegTech Book: The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries in Regulation*, Chichester, Wiley, 2019; Butler T., O'Brien L., "Understanding RegTech for Digital Regulatory Compliance", in Lynn T. *et al.* (a cura di), *Disrupting Finance. FinTech and Strategy in the 21st Century*, Cham, Palgrave Macmillan, 2019, p. 85 ss.; Murphy D., Mueller J., "RegTech: Opportunities for More Efficient and Effective Regulatory Supervision and Compliance", Milken Institute, 2018 https://milkeninstitute.org/sites/default/files/reports-pdf/RegTech-Opportunities-White-Paper-FINAL-.pdf.

[2] Juniper Research, "Whitepaper. How AI and Blockchain are Shaping Regtech", 2023, p. 6, https://www.juniperresearch.com/resources/whitepapers/how-ai-and-blockchain-are-shaping-regtech/. Per uno sguardo alla varietà di proposte presenti sul mercato, cfr. la r*epository online* di Deloitte, *RegTech Universe 2024*, consultabile all'indirizzo https://www.deloitte.com/lu/en/Industries/technology/analysis/regtech-companies-compliance.html.

[3] PwC, "*Smart Compliance*. Un approccio evoluto per la gestione del rischio di non conformità", 2022, p. 12, https://www.pwc.com/it/it/publications/assets/docs/pwc-smart-compliance.pdf.

di dati e informazioni da analizzare[4], ha fatto emergere importanti limiti delle "ordinarie" modalità di svolgimento delle attività di *compliance*.

Le strutture interne appaiono sovente sottodimensionate rispetto all'odierna mole di lavoro; il personale è spesso occupato in attività procedurali ripetitive; le attività di business sono sempre più complesse e interrelate; l'effetto è che i tempi di controllo si allungano e la qualità delle verifiche ne risente[5].

Le imprese sono dunque andate alla ricerca di soluzioni *smart* per porre rimedio a simili inefficienze. La *RegTech* offre, in questo senso, opzioni adattabili a molti contesti[6], rappresentando una risposta 'dal basso' intesa a fronteggiare l'aumento, tra le altre cose, dei costi della *compliance*[7]. I processi aziendali interessati, come si sa, sono oramai i più vari: si va dall'automazione delle attività di acquisizione e analisi della documentazione a fini di controllo, sino a quella dei processi standardizzabili, con analisi multifattoriali del rischio e produzione di *dashboard* dinamiche; dalla *regulatory detection* sino alla *regulatory impact analysis*, avuto riguardo sia alla identificazione automatica delle novità normative, sia alla comparazione e verifica degli impatti su struttura organizzativa e processi; dalle analisi predittive in relazione a rischi operativi e di conformità alla luce di precedenti anomalie, sino alla semplificazione e automatizzazione della creazione di *report*[8].

Bene si comprende, allora, come le potenzialità della tecnologia possano dispiegarsi anche in quel peculiare comparto della *compliance* aziendale volto alla prevenzione del rischio di commissione di reati nell'organizzazione, definito *criminal compliance*, che viene qui in

---

[4] Cfr. Hanley-Giersch J., "RegTech and Financial Crime Prevention", in Barberis J., Arner D.W., Buckley R.P. (a cura di), (2019), *op cit*. L'autrice si richiama sul punto a una ricerca di McKinsey & Company, "Sustainable Compliance: Seven Steps Towards Effectiveness and Efficiency", 2017, https://www.mckinsey.com/business-functions/risk/our-insights/sustainable-compliance-seven-steps-toward-effectiveness-and-efficiency#, secondo cui dall'analisi dell'attività di una grande istituzione finanziaria globale sarebbe emerso che il personale di prima e seconda linea addetto alla *compliance* dedica l'80% del tempo a questioni di rilevanza bassa o moderata, e solo il 20% a questioni critiche ad alto rischio.

[5] Per alcune considerazioni relative alle 'barriere' alla *compliance* aziendale, cfr. Gottschalk P., Hamerton C., *Corporate Compliance. Crime, Convenience and Control*, Cham, Palgrave Macmillan, 2022, p. 75 ss. Si veda anche PwC (2022), *op. cit.*; Monini F., "Non è più solo antiriciclaggio: ai soggetti vigilati vengono chieste decisioni rapide per fronteggiare la vasta area dei *Financial Crimes*", 2019, https://www.protiviti.com/sites/default/files/2022-09/non-e-piu-solo-antiriciclaggio.pdf.

[6] Sarebbe questo uno degli elementi distintivi della *RegTech* rispetto alla *FinTech*, che ha un focus finanziario e si è molto diffusa attraverso le start up. Per un quadro aggiornato, cfr. Baker H.K., Filbeck G., Black K. (a cura di), *The Emerald Handbook of Fintech. Reshaping Finance*, Leeds, Emerald Publishing Limited, 2024; Madir J. (a cura di), *Fintech. Law and Regulation*, III ed., Cheltenham, Edward Elgar Publishing, 2024.

[7] Arner D.W., Buckley R.P., Barberis J., "A FinTech and RegTech Overview: Where We Have Come from and Where We Are Going", in Barberis J., Arner D.W., Buckley R.P. (a cura di), (2019), *op. cit.*

[8] L'elenco delle possibili soluzioni *RegTech* è tratto da PwC, "*RegTech*. La spinta per il nuovo mercato finanziario", 2021, p. 8, https://www.pwc.com/it/it/publications/assets/docs/pwc-regtech.pdf.

considerazione nella versione *digital*[9]. Anzi, non stupirà più di tanto riscontrare che oltre il 30% dei prodotti *RegTech* disponibili è volto ad assistere le imprese per la *compliance* – regolatoria, ma non solo – in materia di *financial crime*[10]; un successo che si lega alla evocata flessibilità di tali strumenti, che si avvalgono, di volta in volta e in base alle esigenze dell'utente, di una selezione o combinazione di tecnologie, per lo più riconducibili alla macro-categoria dell'IA[11].

Il riferimento è, in particolare, al *machine learning* – che nel contesto in esame può supportare la classificazione di documenti in base a specifiche tassonomie –, della biometria comportamentale – che può essere impiegata per l'analisi, appunto, di dati biometrici per autenticare gli utenti e rilevare eventuali attività fraudolente, – dei modelli semantici – in grado di facilitare il c.d. *data mining* e le analisi per conformità e *reporting*.

Anche sul versante penale, la *compliance* digitale, come ricordato, era stata in principio appannaggio soprattutto delle imprese del settore dei servizi finanziari, in considerazione del quadro normativo in evoluzione e della sempre crescente attenzione da parte delle autorità di regolazione[12], richiedendosi capacità di snellire le operazioni e

---

[9] Copiosa è oramai la produzione scientifica sul tema. Nella letteratura internazionale, cfr. Burchard C., "Digital Criminal Compliance", in Engelhart M., Kudlich H., Vogel B. (a cura di), *Digitalisierung, Globalisierung und Risikoprävention: Festschrift für Ulrich Sieber zum 70*, vol. II, Berlino, Duncker & Humblot, 2021, p. 741 ss.; Diamantis M., "The Extended Corporate Mind: When Corporations Use AI to Break the Law", in *North Carolina Law Review*, 2019, vol. 98, p. 893 ss.; Laufer W.S., "The Missing Account of Progressive Corporate Criminal Law", in *New York University Journal of Law & Business*, 2017, vol. 14, p. 71 ss. Nel panorama nazionale, v. in particolare Gullo A., "Compliance", in *Archivio penale web*, 2023, 1, p. 1 ss.; Morgante G., Fiorinelli G., "Promesse e rischi della *compliance* penale digitalizzata", in *Archivio penale web*, 2022, 2, p. 1 ss.; Nisco A., "Riflessi della *compliance* digitale in ambito 231", in *Sistema penale*, 14 marzo 2022; Sabia R., Artificial Intelligence and Environmental Criminal Compliance", in *Revue International de Droit pénal*, 2020, 1, p. 179 ss.; Birritteri E., "*Big Data Analytics* e *compliance* anticorruzione. Profili problematici delle attuali prassi applicative e scenari futuri", in *Diritto penale contemporaneo – Rivista trimestrale*, 2019, 2, p. 289 ss.; Selvaggi N., "Dimensione tecnologica e *compliance* penale: un'introduzione", in Lupària L., Marafioti L., Paolozzi G. (a cura di), *Dimensione tecnologica e prova penale*, Torino, Giappichelli, 2019, p. 217 ss.

[10] KPMG, "Unlocking the Potential of RegTech", 2023, p. 9, https://assets.kpmg.com/content/dam/kpmg/ie/pdf/2023/02/ie-regtech-potential.pdf.

[11] PwC (2021), *op. cit.* Sugli impieghi dell'IA per la gestione del rischio, si veda anche Deloitte, "AI and Risk Management. Innovating with Confidence", 2018, https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/financial-services/deloitte-uk-ai-and-risk-management.pdf.

[12] Si è, peraltro, andata consolidando una branca ulteriore, quella della *SupTech*, ossia l'uso di tecnologie innovative da parte delle autorità di vigilanza: PwC, "*SupTech*: l'innovazione del settore finanziario a supporto del Regolatore", 2021, https://www.pwc.com/it/it/publications/assets/docs/SupTech.pdf; Broeders D., Prenio J., *Innovative Technology in Financial Supervision (SupTech) – The Experience of Early Users*, 2018, https://www.bis.org/fsi/publ/insights9.htm. La *SupTech* è espressamente considerata nel Piano strategico 2022-2024 di Consob, così come è sperimentata da Banca d'Italia (per approfondire, cfr. https://www.bancaditalia.it/pubblicazioni/altri-atti-convegni/2024-indagine-fintech/Vigilanza-Giacona.pdf; si veda anche lo studio di Coelho R., De Simoni M., Prenio J., "Suptech Applications for Anti-Money Laundering", pubblicato nel n. 14/2019 dei *Quaderni dell'antiriciclaggio. Analisi e studi* dell'UIF, https://uif.bancaditalia.it/pubblicazioni/quaderni/2019/quaderno-14-2019/index.html?dotcache=refresh.

mantenere, al contempo livelli di controllo adeguati[13]. Tali enti sono stati chiamati progressivamente a farsi carico non solo di obblighi nei consueti ambiti – *anti-money laundering* (AML), *know your customer* (KYC), *countering terrorist financing* (CTF) –, ma anche ad adottare più ampi *framework* di prevenzione di illeciti ulteriori. Si parla, al riguardo di *anti financial crime* (AFC), che può includere reati in materia societaria, di cybersicurezza, contro la pubblica amministrazione[14].

La diffusione poi, negli ultimi decenni, di regimi di responsabilità da reato degli enti a livello globale[15] ha costituito un fattore determinante per l'allargamento del bacino di attori societari interessati a migliorare i propri assetti di *crime prevention*. Secondo un trend evidente in molti ordinamenti, sempre più spesso l'adozione di misure di *compliance* diventa un fattore in grado di schermare – seppur con diversità di intensità ed effetti – l'impresa da possibili ricadute sul piano della responsabilità penale, o comunque punitiva[16]. Emblematico il caso dell'ordinamento italiano: il noto D.Lgs. n. 231/2001, costruito attorno al modello organizzativo quale architrave, e tangibile output, delle attività di prevenzione, è stato un importante volano per la diffusione della *compliance* nel nostro Paese[17].

Considerati i riflessi in punto di *corporate liability*, appare quindi chiaro l'interesse per le imprese a dotarsi di presidi efficaci, in grado di individuare e gestire il rischio-reato anche mediante l'ausilio delle migliori tecnologie.

Si delinea, quindi, un orizzonte in cui si stagliano, da un lato, le promesse della tecnologia per supportare e potenziare le attività delle aziende, in specie nella gestione del carico regolatorio, anche penale; e, dall'altro, si profilano – per le ipotesi di *non-compliance* e verificazione di reati nell'impresa ricollegabili all'impiego di tali sistemi intelligenti – rischi sanzionatori che, nelle principali giurisdizioni nazionali, attingono direttamente gli enti.

Da questo specifico angolo di osservazione, obiettivo del presente contributo è riflettere sullo stato dell'arte dei rapporti tra *compliance*

---

[13] Accenture, "Getting Ahead of Financial Crime with AI", 2018, p. 2

[14] Per un riferimento a tali aree si veda, ad esempio, l'*Handbook* della UK Financial Conduct Authority (FCA), l'organo di vigilanza e controllo dei mercati finanziari del Regno Unito: https://www.handbook.fca.org.uk/handbook. Sul tema, cfr. anche ACCA, EY, "Economic Crime in a Digital Age", 2020, https://www.accaglobal.com/in/en/professional-insights/risk/Economic_Crime_Digital_Age.html.

[15] In argomento, cfr. Sabia R., *Responsabilità da reato degli enti e paradigmi di validazione dei modelli organizzativi. Esperienze comparate e scenari di riforma*, Torino, Giappichelli, 2022; Mongillo V., *La responsabilità penale tra individuo ed ente collettivo*, Torino, Giappichelli, 2018.

[16] Sabia R. (2022), *op. cit*.

[17] Così Mongillo V., "Presente e futuro della *compliance* penale. Riflessioni a margine di Manacorda S., Centonze F. (a cura di), *Corporate Compliance on a Global Scale. Legitimacy and Effectiveness"*, 2022, in *Sistema penale*, 11 gennaio 2022, p. 2.

penale e utilizzo delle tecnologie per la prevenzione di reati. Nelle pagine che seguono, si muoverà, anzitutto, da alcune possibili applicazioni di interesse, quali l'IA per la *data analytics* e la tecnologia *blockchain* (paragrafo 2), per poi procedere a una verifica dell'impatto di simili innovazioni nella *compliance* penale sul delicato terreno della responsabilità da reato degli enti, da ultimo anche alla luce del Regolamento europeo sull'intelligenza artificiale (*AI Act*, paragrafo 3). Nella parte conclusiva, si getterà lo sguardo in ottica comparata all'esperienza del Department of Justice statunitense, che ha recentemente incluso l'uso dell'IA da parte delle imprese tra i rischi emergenti da considerare nella valutazione dei *corporate compliance program* (paragrafo 4).

2. La digitalizzazione della *compliance* penale: alcune possibili applicazioni

Come rimarcato, "sorprendente" è la varietà di possibili applicazioni[18] per gestire i processi interni e di conformità normativa: l'IA riveste senz'altro un ruolo chiave, ma il novero degli strumenti disponibili si è nel tempo arricchito, con la *blockchain* e gli *smart contract* che pure si sono imposti all'attenzione[19].

Le ragioni d'interesse verso i menzionati strumenti, come già rilevato, si legano al fatto che protagonisti delle attività di *regulatory compliance* sono i dati, i flussi finanziari, le informazioni; e il tema travalica, in verità, la dimensione privata, riguardando anche il settore pubblico, ove, per effetto anche della normativa in tema di obblighi di trasparenza e appalti pubblici, l'amministrazione ha ampliato notevolmente il proprio patrimonio di dati[20].

Sul versante delle imprese, la scelta di prevenire e gestire il rischio legato alla commissione di reati ricorrendo alle nuove tecnologie può presentare rilevanti conseguenze, in almeno due direzioni. La digitalizzazione può, *in primis*, contribuire a rendere più efficienti le attività di *risk assessment e management*, supportando dunque l'ente nella costruzione e attuazione del *compliance program*; in secondo luogo, però, introdurre simili tecnologie – e particolarmente quelle di IA basate sul *machine learning* – potrebbe innescare per i soggetti collettivi nuovi rischi, ad esempio nelle ipotesi in cui il ritrovato tecnologico fallisca nell'obiettivo di *detection* dell'illecito, o laddove il suo errato funzionamento agevoli la commissione del reato.

---

[18] Morgante G., Fiorinelli G. (2022), *op. cit.*

[19] Tali profili sono stati oggetto di considerazione anche in Gullo A., "I modelli organizzativi", in Lattanzi G., Severino P. (a cura di), *Responsabilità da reato degli enti*, vol. I, *Diritto sostanziale*, Torino, Giappichelli, 2020, p. 284 ss., nonché più di recente, in Gullo A. (2023), *op. cit.*

[20] Gullo A. (2023), *op. cit.*

Assumeremo come riferimento e principale 'caso studio' il sistema italiano *ex* D.Lgs. n. 231/2001, soffermandoci dapprima sulle 'luci': il binomio modello organizzativo-*digital criminal compliance* mostra, infatti, numerosi esempi d'uso promettenti.

Gli algoritmi sono in grado di supportare l'elaborazione di una enorme quantità di dati (i c.d. *Big Data*), con possibili intuitivi benefici per tutti gli *step* di progettazione e gestione del rischio: certamente, nel momento di individuazione delle attività nel cui ambito possono essere commessi reati, nonché nella definizione e adozione delle specifiche cautele volte al contenimento dei rischi identificati, e altresì nell'aggiornamento del modello organizzativo.

Per l'impresa che aspiri alla validazione giudiziale del modello organizzativo in caso di verificazione di un reato presupposto, l'efficace processamento dei dati, l'affidabile tracciabilità dei flussi finanziari e un efficiente circuito informativo sono invero obiettivi essenziali sia nel momento della costruzione dell'assetto di prevenzione e dell'individuazione delle attività nel cui ambito possono essere commessi reati, sia una volta che il modello organizzativo trovi attuazione (diversamente, l'assenza di trasparenza e adeguata procedimentalizzazione potrebbe indiziare colpa di organizzazione).

Tra le aree di utilizzo più frequente di tali *tool* al servizio della *compliance* penale digitale, senza pretesa di esaustività, si ricordano il *machine learning* e l'*advanced analytics* in grado, appunto, di condurre analisi su interi comparti documentali (ad esempio e-mail) e ricercare comportamenti anomali[21]; di svolgere verifiche su adempimenti e di approntare *report* in *real time* per il top management e gli organi di controllo (ad esempio l'OdV), circa rilevati indicatori di allarme (c.d. *red flag*, che possono in ipotesi emergere anche durante lo svolgimento di una procedura); di realizzare la *due diligence* delle terze parti anche attraverso l'*intelligence* su fonti aperte[22]; di procedimentalizzare le attività aziendali conformemente agli standard normativi (ad esempio includendo obiettivi, soglie, divieti), così limitando tecnicamente la possibilità d'agire degli individui[23]; di fornire indicazioni – una sorta

---

[21] Per le casistiche qui richiamate cfr. Birritteri E. (2019), *op. cit.* Si rileva nel report di ACCA, EY (2020), *op. cit.,* che anche i test descrittivi basati su regole – *analytics* facili da implementare in quanto si basano su condizioni e politiche predefinite – utilizzando 'dati storici con test analitici ponderati semplici e complessi', possono migliorare l'identificazione delle aree di rischio e produrre avvisi quando viene soddisfatta una specifica condizione. Il report evidenzia, anzi, che è la tecnica di *forensic data analytics* più comunemente utilizzata in azienda; ad esempio, scatta un allarme nel caso in cui un dipendente presenti una spesa da rimborsare per un importo superiore rispetto a quanto previsto dalla *policy* di rimborso predefinita.

[22] Con riferimento ai *software* di *decision intelligence* e *open source intelligence (OSINT)*, cfr. D'Agostino L., "*Criminal compliance* e nuove tecnologie", in *Diritto penale contemporaneo – Rivista trimestrale,* p. 9 e p. 15 ss.

[23] Morgante G., Fiorinelli G. (2022), *op. cit.,* in cui si trova l'esempio, rispetto alla gestione delle disposizioni di pagamento in uscita dall'ente, di presidi digitali che potrebbero "non soltanto

di *predictive policing* privato – su eventuali futuri comportamenti illeciti dei dipendenti[24].

Anche rispetto a un tempestivo aggiornamento del modello organizzativo, vengono in considerazione strumenti a supporto dei mutamenti normativi e/o aziendali da recepire da parte delle funzioni/livelli aziendali competenti; nonché, in termini più incisivi ma, ci sembra, anche più prospettici, sistemi che possano consentire una sorta di 'auto-aggiornamento' del modello organizzativo, sulla base di un previo "addestramento" legato all'esperienza pregressa e sui risultati del *continuous monitoring*[25].

È quindi chiaro che l'IA cambierà "radicalmente le metodiche e le pratiche della *compliance* penale e la progettazione dei sistemi di controllo interno alle imprese"[26], supportando *ex-ante* la valutazione del rischio e, in quanto *smart technology* in grado di apprendere durante il processo, identificando nuovi indicatori e modelli di comportamento legati ad attività non conformi e sospette[27], così da migliorare le proprie capacità predittive su eventi futuri. Inoltre, l'IA può fornire indicazioni puntuali anche per l'analisi *ex-post* delle cause di eventuali 'non conformità', e la correzione/revisione di eventuali deficienze del modello organizzativo[28].

Non si può poi escludere che, in taluni settori, l'impiego dell'IA possa contribuire a integrare quelle *best practice* condivise in grado di legittimare una presunzione relativa superabile dal giudice con motivazione rafforzata[29].

Non meno d'impatto sono le potenzialità della *blockchain*, per le sue caratteristiche di immodificabilità, decentralizzazione e resilienza[30].

---

consentire di tracciare o monitorare in tempo reale le transazioni e di verificarne in modo automatizzato la corrispondenza con disposizioni di acquisto e fatture passive, ma [...] soprattutto rendere tecnicamente impossibile (e, dunque, impedire) l'esecuzione di pagamenti anomali o difformi rispetto ai protocolli aziendali: inabilitando, ad esempio, l'effettuazione di bonifici a favore di destinatari che non risultino già censiti e approvati nell'anagrafe aziendale, con l'effetto, dunque, di ridurre, se non addirittura eliminare, il rischio di comportamenti appropriativi, distrattivi, o financo corruttivi".

[24] In questi termini, ancora Morgante G., Fiorinelli G. (2022), *op. cit.*

[25] Morgante G., Fiorinelli G. (2022), *op. cit.,* richiamano sul punto PwC, "Il Modello 231/01 tra innovazioni normative e tecnologiche", 2021, p. 8 ss., https://www.pwc.com/it/it/publications/docs/pwc-modello-231-01-normative-tecnologie.pdf.

[26] Mongillo V., "Responsabilità da reato degli enti e crimini connessi all'intelligenza artificiale: tecniche giuridiche di intervento e principali ostacoli", in *Archivio penale web*, 2024, 2, p. 3.

[27] Cfr., in tal senso, ad esempio, Accenture (2018), *op. cit.*

[28] Gullo A. (2020), *op. cit.*

[29] Gullo A. (2023), *op. cit.* Il riferimento è qui alla proposta di Piergallini C., "Premialità e non punibilità nel sistema della responsabilità degli enti", in *Diritto penale e processo*, 2019, 4, p. 536. Sul terreno della *compliance* penale digitale la tesi è stata richiamata da D'Agostino L. (2023), *op. cit.*, nonché da Birritteri E. (2019), *op. cit.* La prospettiva è da ultimo menzionata anche da Fimiani L., "La tecnologia nel sistema penale: dalla giustizia predittiva alle problematiche sull'utilizzo della "IA" per prevenire episodi criminosi", in *Discrimen*, 18 novembre 2024, p. 10 s.

[30] Le considerazioni che seguono sull'uso della *blockchain* in ambito '231' sono riprese da Gullo A.

Tale tecnologia, come noto, prevede che le transazioni avvengano all'interno di un registro distribuito, strutturato in blocchi, con un processo di validazione di ciascuna operazione diffuso tra tutti i nodi della rete; la modifica delle transazioni è possibile solo al raggiungimento del consenso tra i nodi.

Si è prefigurata la possibilità di una *blockchain* privata e *permissioned*[31], ossia di un sistema costituito da nodi coincidenti unicamente con realtà interne dell'ente, decentralizzato sotto il profilo della gestione e inserimento dei dati, e centralizzato quanto a direzione dei nodi – ciò che assicurerebbe all'impresa di conservarne il governo (es. rispetto all'ammissione e amministrazione dei nodi della rete, alla diffusione e disponibilità delle informazioni etc.).

I possibili vantaggi, ove si ricomprendessero in tale infrastruttura come 'nodi' singole funzioni, organi gestori nonché di controllo (si pensi al collegio sindacale e all'OdV), si legano al fatto che questi avrebbero, da un lato, accesso al compendio informativo, con evidenti implicazioni per la capillarità del menzionato controllo; dall'altro, interventi sui dati (es. cancellazione) – proprio perché scritti su un registro decentralizzato – potrebbero avvenire solo se validati da tutti i nodi (in ipotesi, se l'OdV rappresentasse un nodo della *blockchain*, nessuna informazione potrebbe essere alterata senza il suo espresso consenso).

Il meccanismo, quindi, permettendo la tracciabilità delle operazioni e la conservazione e immutabilità del dato, si candida a utili impieghi sia in ottica anticipata, per rafforzare la *compliance* preventiva dell'impresa, ma anche in prospettiva postuma in occasione di eventuali *internal investigation*[32], nonché dell'interlocuzione con l'autorità giudiziaria, in punto di ricostruzione di possibili violazioni e di *self-reporting* dell'ente.

Peraltro, è possibile anche una combinazione sinergica e integrazione di diverse tecnologie (IA, *blockchain* e *smart contract*, ossia contratti che, al verificarsi delle condizioni scritte nel codice, sarebbero

---

(2023), *op. cit.,* nonché Gullo A. (2020), *op. cit.* Sulla *blockchain* in termini generali cfr. Anjum A., Sporny M., Sill A., "Blockchain Standards for Compliance and Trust", in *IEEE Cloud Computing*, 2017, 4, p. 84 ss.; Zhang W., Yuan Y., Hu Y. *et al.*, "Blockchain-Based Distributed Compliance in Multinational Corporations' Cross-Border Intercompany Transactions. A New Model for Distributed Compliance Across Subsidiaries in Different Jurisdictions", in Arai K., Kapoor S., Bhatia R. (a cura di), *Advances in Information and Communication Networks. Proceedings of the 2018 Future of Information and Communication Conference (FICC)*, vol. 2, Cham, Springer, 2018, p. 304 ss.

[31] Letizi M., Soana G., "Le potenzialità del modello di *corporate compliance* integrato basato sulla tecnologia *Blockchain*", in *Norme e Tributi Plus, Il Sole 24 ore,* 21 dicembre 2020, cui si rinvia anche per una disamina sui caratteri della *blockchain* applicata alla *corporate compliance* aziendale. L'impiego della *blockchain* è peraltro di sicuro interesse in molteplici ambiti, incluso quello degli appalti e della destinazione di fondi pubblici: v. Gullo A. (2023), *op. cit.*

[32] Tocca questo profilo Nisco A. (2022), *op. cit.*

suscettibili di esecuzione automatica)[33]; con l'effetto di migliorare le complessive *performance* del sistema di *compliance* e di potenziare significativamente la resilienza e capacità d'intervento dell'organizzazione.

3. IA e prevenzione dei reati: i riflessi sul piano della responsabilità da reato degli enti

I numerosi ed evidenti vantaggi di cui si è detto non debbono, tuttavia, mettere in secondo piano i profili critici legati alla digitalizzazione della *compliance*, e particolarmente di quella penale.

In primo luogo, è bene ricordare che anche nel contesto aziendale le nuove tecnologie, e l'IA specialmente per le sue caratteristiche, sollevano problemi di ordine generale[34] – rischi etici, sociali o economici[35] – che altrove sono già stati esaminati, e che ci limitiamo, qui, solamente a richiamare[36]: quale presupposto per il funzionamento dei sistemi avanzati di IA, il tema della qualità dei dati, sulla cui base gli algoritmi identificano *pattern* e assumono decisioni (*i.e.* l'assenza di ingenti set di dati di alta qualità[37] si ripercuote sulla qualità di tali decisioni); quello della intellegibilità, *explainability* e trasparenza, specie nei sistemi più complessi – c.d. *black box effect*[38] – che rappresenta oggi, anche alla luce dei recenti approdi normativi in sede europea[39], un profilo di assoluto rilievo per le organizzazioni (si pensi alle difficoltà di convalidare gli output e, eventualmente, rappresentare alle autorità come sono state prese le decisioni)[40]; l'impatto che l'IA può avere sul personale dell'azienda e sulla riorganizzazione del lavoro

---

[33] Gullo A. (2023), *op. cit.*

[34] Tali problemi rappresenterebbero un ostacolo all'adozione di simili tecnologie in ambito *corporate* su larga scala: cfr. Accenture (2018), *op. cit.* Si è anzi detto che è comprensibile che i vertici aziendali esitino a ricorrere "all'uso dell'IA per le attività regolamentate nella loro organizzazione, a meno che non ritengano di avere una comprensione significativa della tecnologia", Deloitte (2018), *op.cit.*

[35] Per uno sguardo d'insieme degli orizzonti tecnici, di *policy* ed economici legati all'uso dell'IA, si veda OECD, "Artificial Intelligence in Society", 2019, https://doi.org/10.1787/eedfee77-en; Floridi L., Cowls J., Beltrametti M. *et al.*, "AI4People – An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations", in *Minds & Machines*, 2018, 28, p. 689 ss.

[36] Sabia R. (2020), *op. cit.;* Gullo A. (2023), *op. cit.* Per un quadro dei rischi 'vecchi' e 'nuovi' legati alla digitalizzazione della *compliance*, v. Mozzarelli M., "Digital Compliance: The Case for Algorithmic Transparency", in Centonze F., Manacorda S. (a cura di), *Corporate Compliance on a Global Scale. Legitimacy and Effectiveness*, Cham, Springer, 2022, p. 262 ss.

[37] Deloitte (2018), *op.cit.*

[38] Per una lettura critica sull'uso dei *Big Data* in ambito *corporate*, Pasquale F., *The Black Box Society: The Secret Algorithms That Control Money and Information,* Harvard, Harvard University Press, 2015.

[39] V. *infra* in questo paragrafo.

[40] Accenture (2018), *op. cit.*

che potrebbe seguire all'adozione di questi sistemi; la problematica della cybersicurezza dell'IA.

Sul versante più strettamente giuridico, l'impiego delle tecnologie può avere risvolti delicati, in particolare, ove si presti a consentire un controllo sui dipendenti e/o a rilevarne eventuali comportamenti 'devianti'.

Le principali questioni, cui pure la dottrina ha già dedicato attenzione[41], attengono, a seconda dei casi, al possibile "controllo occulto" sui lavoratori – si profilano frizioni con la disciplina lavoristica, in riferimento alle previsioni che richiedono particolari presidi per l'installazione di strumenti di controllo a distanza per le finalità previste dalla normativa di settore[42] –, ai risvolti sulla protezione dei dati personali – l'art. 22 GDPR, come noto, vieta l'adozione di decisioni basate unicamente sul trattamento automatizzato di dati[43], all'incidenza sulle garanzie difensive – nella eventualità che le già ricordate *internal investigation* aziendali, in assenza di un chiaro quadro regolatorio, si avvalgano di tali tecnologie facendo emergere risultanze potenzialmente pregiudizievoli per il singolo[44].

Soffermandoci, invece, sugli aspetti che attengono più direttamente alla struttura della responsabilità dell'ente, la *digital criminal compliance* solleva diversi interrogativi. La capacità prestazionale di tali tecnologie – in grado di far emergere anomalie e individuare rischi che, diversamente, non sarebbe stato possibile identificare, o per lo meno non con il medesimo livello di accuratezza – potrebbe portare, in prospettiva, a rivedere gli obiettivi di prevenzione richiesti all'ente.

A fronte di ritrovati tecnologici con capacità superiori a quelle umane, un primo tema attiene allo standard cautelare di riferimento: se si possa ancora parlare – come molti ritengono con riferimento alla "*compliance* analogica", muovendo in particolare dalla natura delle cautele qui in considerazione – di una realistica riduzione significativa

---

[41] Per una panoramica dei diversi problemi, cfr. Birritteri E. (2019), *op. cit.*; Morgante G., Fiorinelli G. (2022), *op. cit.*

[42] Il referente normativo, nello scenario interno, è l'art. 4 dello Statuto dei lavoratori. Per un approfondimento, v. Birritteri E., "Controllo a distanza del lavoratore e rischio penale", in *Sistema penale*, 16 febbraio 2021; Nisco A., "Prospettive penalistiche del controllo a distanza sull'attività lavorativa nell'attuale contesto normativo e tecnologico", *ivi*, 20 dicembre 2021.

[43] Tocca questo aspetto Birritteri E. (2019), *op. cit.*

[44] Per un quadro critico sulle *internal investigation* si veda Mancuso E.M., "Le investigazioni interne nel sistema processuale italiano: tra vuoto normativo e prassi applicative incerte", in Centonze F., Mantovani M. (a cura di), *La responsabilità «penale» degli enti. Dieci proposte di riforma*, Bologna, Il Mulino, 2016, p. 217 ss.; Nicolicchia F., "*Corporate Internal Investigations* e diritti dell'imputato del reato presupposto nell'ambito della responsabilità «penale» degli enti: alcuni rilievi sulla base della «lezione americana»", in *Rivista trimestrale di diritto penale dell'economia*, 2014, 3-4, p. 781 ss.; si veda anche il volume curato da Centonze F., Giavazzi S., *Internal Investigations. Best practices e istanze di regolamentazione,* Torino, Giappichelli, 2021.

del rischio, oppure se questi strumenti potranno in futuro condurre, almeno in certi settori, a un vero e proprio azzeramento del rischio[45].

Nella medesima direzione, ci si potrebbe domandare se la condotta organizzativa in capo all'ente sia da ritenersi esigibile, ove si discuta di tecnologie che siano, in ipotesi, alla portata anche di medie o medio-piccole realtà imprenditoriali; né rimarrebbe fuori da simili considerazioni il ruolo, in prospettiva, dell'OdV, dato che la digitalizzazione della *compliance* comporterebbe, come detto, una verosimile estensione e un maggiore livello di analiticità del controllo richiesto[46].

È stato sottolineato in chiave critica che "la pretesa di [...] maggiore effettività, avanzata da queste tecnologie, è destinata a incidere sul formarsi di *best practice*", e ciò potrebbe finire per incidere anche sulla validazione giudiziale dei modelli organizzativi "che non adottano misure tecnologiche (ritenute non eludibili), o adottano sistemi (considerati) poco performanti"[47]. C'è quindi da chiedersi – considerando la ricordata crescita della *RegTech*, con dati di interesse anche per il mercato italiano[48] – se l'innesto della tecnologia nella *compliance* penale possa mutare i caratteri della colpa di organizzazione e le scansioni del relativo accertamento, nel caso di possibili reati presupposto la cui integrazione risulti agevolata dal cattivo funzionamento dell'algoritmo[49].

Come si sa, nell'impianto del D.Lgs. n. 231/2001, la colpa di organizzazione, quale elemento costitutivo dell'illecito dell'ente[50] nella visione oramai consolidata, si radica nella mancanza di presidi, o nell'insufficienza/inadeguatezza di quelli approntati. La prassi pare orientarsi nel senso di ritenere che la colpa di organizzazione debba essere sempre riscontrata dal giudice, ripercorrendo le cadenze tipiche dell'accertamento della colpa individuale[51]; pertanto, l'assenza

---

[45] Gullo A. (2020), *op. cit.*

[46] Gullo A. (2020), *op. cit.*

[47] Nisco A. (2022), *op. cit*. Sull'impatto delle nuove tecnologie in punto di verifica dell'idoneità dei modelli, v. Selvaggi N. (2019), *op. cit.*

[48] Cfr. ad esempio, "Insurtech, in Italia il 2024 annata record per gli investimenti in intelligenza artificiale", 2024, https://www.corrierecomunicazioni.it/digital-economy/insurtech-in-italia-il-2024-annata-record-per-gli-investimenti-in-intelligenza-artificiale/.

[49] Sul punto, cfr. Birritteri E. (2019), *op. cit.*; Sabia R. (2020), *op. cit*.

[50] Si veda, per tutti, De Simone G., *Persone giuridiche e responsabilità da reato. Profili storici, dogmatici e comparatistici*, Pisa, Edizioni ETS, 2012, p. 394 ss.

[51] V. la ricostruzione svolta dalla Cassazione nel *leading case Impregilo bis*: Cass. pen., sez. VI, 11 novembre 2021 (dep. 15 giugno 2022), n. 23401, in *Sistema penale*, 20 giugno 2022; v. in particolare le annotazioni di Piergallini C., "Una sentenza ''modello'' della Cassazione pone fine all'estenuante vicenda ''Impregilo''", in *Sistema penale*, 27 giugno 2022; Fusco E., Paliero C.E., "L'"happy end'' di una saga giudiziaria: la colpa di organizzazione trova (forse) il suo tipo", *ivi*, 2022, 9, p. 115 ss.; Bianchi D., "Verso un illecito corporativo personale. Osservazioni 'umbratili' a margine d'una sentenza 'adamantina' nel 'magma 231'", *ivi*, 14 ottobre 2022; Merlo A., "Il D.Lgs. 231/01 preso sul serio: la Cassazione scrive l'ultimo capitolo della saga 'Impregilo'", in *Foro italiano*, 2022, 11, II, col. 669 ss.; Centonze F., "Il crimine dell'"attore decisivo'', i limiti della *compliance* e

del modello organizzativo non dovrebbe determinare un automatico addebito, al più potendo indiziare profili di tale colpa[52], e sempre che le prescrizioni cautelari non siano state osservate – anche in considerazione delle peculiarità dell'ente – ricorrendo a differenti modalità preventivo-organizzative.

L'impressione – almeno *de iure condito* – è che l'impiego di 'agenti intelligenti' da parte dell'impresa per le proprie attività di *risk-assessment* e *risk-management* in campo penale non incida sull'impianto appena tratteggiato. Richiamando quanto già evidenziato con riguardo ai limiti, intrinseci e strutturali, circa la prevedibilità dei risultati cui può giungere il sistema di IA, un errore dell'algoritmo – in fase di *detection*, o di *monitoring* del rischio – non può determinare, di per sé, la responsabilità da reato dell'ente che ne faccia uso. Poiché nella normalità dei casi tale *tool* sarà stato reperito sul mercato, il fallimento tecnologico dovrà, con ogni probabilità, farsi risalire a fasi antecedenti (progettazione, etc.) la comprensione del difetto organizzativo travalicando le capacità del singolo ente che si è affidato a operatori altamente specializzati[53].

La *organisational fault* non può che fondarsi, anche in tale contesto, su carenze organizzative 'proprie' del soggetto collettivo che scelga di digitalizzare le attività di *criminal compliance* – es. non aver previsto adeguata supervisione umana, o non aver predisposto procedure interne per valutare l'output algoritmico, ed eventualmente per prendere decisioni che si discostino da esso. Se l'ente ha adottato e implementato un modello organizzativo ben strutturato, che ricomprenda anche una corretta valutazione/supervisione dei rischi correlati all'impiego delle tecnologie prescelte, sembra difficile rinvenire spazi per un rimprovero colposo. Appaiono altresì quanto meno futuribili prospettive di responsabilizzazione dell'ente per la mera scelta di affidarsi integralmente, per tali finalità preventive, a un certo specifico sistema *tech*[54]; almeno per quanto concerne l'IA, come a breve si dirà, la necessità dell'intervento umano, l'*assessment* dei rischi legati al suo

---

la prova ''certa'' della colpa di organizzazione – riflessioni a margine della sentenza ''Impregilo'', in *Cassazione penale*, 2022, p. 4383 ss.; De Simone G., "Si chiude finalmente, e nel migliore dei modi, l'annosa vicenda Impregilo", in *Giurisprudenza italiana*, 2022, p. 2758 ss.; Mongillo V., "La colpa di organizzazione: enigma ed essenza della responsabilità ''da reato'' dell'ente collettivo", in *Cassazione penale*, 2023, p. 714 ss.

[52] In giurisprudenza si è sostenuto che l'assenza del modello organizzativo, la sua inidoneità o la sua inefficace implementazione non siano, di per sé, elementi costitutivi dell'illecito dell'ente, pur integrando una circostanza idonea a dimostrare la sussistenza della colpa di organizzazione che deve, comunque, essere provata dall'accusa: cfr. Cass. pen., sez. IV, 15 febbraio 2022 (dep. 10 maggio 2022), n. 18413, con nota di Apuzzo L., in *Rivista trimestrale di diritto penale dell'economia,* 2022, p. 363 ss.

[53] Nisco A. (2022), *op. cit*.

[54] Selvaggi N. (2019), *op. cit.;* Severino P., "Intelligenza artificiale e diritto penale", in Ruffolo U. (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, Giuffrè, 2020, p. 538.

impiego e i correlati obblighi sono capisaldi del nuovo Regolamento europeo sull'intelligenza artificiale.

Né si qualifica come una reale alternativa, nella sua configurazione attuale, il paradigma dell'autonomia (art. 8 D.Lgs. n. 231/2001). La giurisprudenza ritiene necessario l'accertamento di un fatto tipico, antigiuridico e altresì *colpevole* commesso da un individuo appartenente alla compagine societaria; in dottrina si è evidenziata anche l'importanza di ricostruire quale sia la categoria soggettiva di appartenenza (apicale/sottoposto), per i correlativi riflessi sull'ente *ex* artt. 6-7 del Decreto[55].

Inoltre, si sostiene la necessità di individuare, anche in caso di autore-persona fisica non identificato o non imputabile, una "correlazione funzionale tra la carente organizzazione e il reato presupposto, che replichi le fattezze del giudizio per colpa"[56]: si è osservato che lo schema *ex* art. 8 D.Lgs. n. 231/2001 avrebbe natura mista, dal momento che la mancata individuazione dell'autore dipenderebbe dalla mancanza o inefficacia di assetti organizzativi dell'ente (nel "disegno organizzativo delle funzioni aziendali" o "nell'ambito delle singole procedure di contenimento del rischio-reato")[57]. Riemergerebbero, in tal senso, le difficoltà ermeneutiche già segnalate.

E vale anche la pena ricordare, come altrove si è avuto modo di approfondire, che la questione dell'ascrizione della responsabilità all'ente per *algorithmic misconduct* si pone, anche nell'esperienza comparata, evocando problemi simili, avuto riguardo ai principali modelli di *corporate criminal liability*[58].

---

[55] Per un commento alla disposizione, Bellacosa M., "Articolo 8. Autonomia della responsabilità dell'ente", in Levis M., Perini A. (diretto da), *Il 231 nella dottrina e nella giurisprudenz*a a vent'anni dalla sua promulgazione, Bologna, Zanichelli, 2021, p. 292 ss.; v. altresì Consulich F., "Il principio di autonomia della responsabilità dell'ente. Prospettive di riforma dell'art. 8", in *La responsabilità amministrativa delle società e degli enti*, 2018, 4, p. 197 ss.; D'Arcangelo F., "Il principio di autonomia della responsabilità dell'ente", in Piva D. (a cura di), *La responsabilità degli enti ex D.Lgs. n. 231/2001 tra diritto e processo*, Torino, Giappichelli, 2021, p. 308 ss.; Pelissero M., "La responsabilità dell'ente tra dipendenza da reato e autonomia", in Cornacchia L., Crespo E.D. (a cura di), *Responsabilità da reato degli enti collettivi. Profili dogmatici e politico-criminali a oltre vent'anni dal D.Lgs. 231/2001*, Torino, Giappichelli, 2023, p. 29 ss.

[56] Piergallini C., "Intelligenza artificiale: da 'mezzo' ad 'autore' del reato?", in *Rivista italiana di diritto e procedura penale*, 2020, p. 1756, richiamando sul punto, per la ricostruzione del nesso ascrittivo nell'art. 8, Paliero C.E., "La società punita: del come, del perché, e del per cosa", in *Rivista italiana di diritto e procedura penale*, 2008, p. 1541 ss.; *Id.*, "La colpa di organizzazione tra responsabilità collettiva e responsabilità individuale", in *Rivista trimestrale di diritto penale dell'economia*, 2018, 1-2, p. 216 ss.

[57] Piergallini C. (2020), *op. cit.*

[58] In particolare, in ordinamenti, come il Regno Unito, basati sulla regola ascrittiva della *identification – i.e.* solo se chi commette il reato è un soggetto in posizione di *top management*, l'elemento oggettivo e quello mentale a costui riferibili si considerano 'propri' (anche) dell'ente – non pare possibile 'sostituire' l'algoritmo al soggetto in posizione super-apicale (anche perché la tecnologia usualmente supporta attività di *compliance* svolte, per lo più, ai livelli intermedi della gerarchia); e lo stesso si può dire rispetto agli schemi emersi più di recente, come il c.d. *failure to prevent model* che, pur innestandosi su *corporate offence* a dimensione

L'analisi del *framework* normativo di riferimento, peraltro, non può oggi non guardare, come accennato, alle novità recate dalla recente approvazione dell'*AI Act*[59], destinate ad avere un forte impatto sulle attività di *corporate compliance* e sulla strutturazione dell'analisi e gestione dei rischi, compreso quello penale.

Il Regolamento europeo, sposando ancora una volta l'approccio basato sul rischio[60], introduce obblighi diversi in capo a vari attori della catena del valore dell'IA, tra cui si annoverano non solo i fornitori, importatori, distributori etc., ma anche coloro che utilizzano tali sistemi – i c.d. *deployer*, definiti come persone fisiche o giuridiche, autorità pubbliche, agenzie e altri organismi che utilizzino un sistema di IA sotto la propria autorità (con esclusione degli impieghi personali non professionali)[61].

Detti obblighi sono diversamente modulati, in ottica di proporzione, in base non solo al tipo di attore coinvolto, ma anche – ed è questo un pilastro della normativa – in base al livello di rischio del singolo sistema in considerazione, secondo la classificazione operata dal Regolamento. Al livello di rischio inaccettabile, corrispondono le pratiche vietate; per i sistemi ad alto rischio, si prevedono specifici requisiti e specifici obblighi in capo agli operatori; per i sistemi a rischio limitato, sono stabiliti obblighi di trasparenza[62].

Dunque, maggiore è il rischio che il loro l'utilizzo può comportare per l'utente, più stringente risulterà la relativa regolamentazione: all'evidenza, la categoria più problematica appare quella dei sistemi ad alto

---

"strutturalmente collettiva", sul piano 'fenomenico' richiedono comunque la commissione di un reato da parte di una persona fisica. Anche se si guarda al modello della *vicarious liability*, quale regola d'imputazione generale negli Stati Uniti, l'ingresso sulla scena degli algoritmi mette in crisi i paradigmi tradizionali, che poggiano sull'elemento mentale dell'agente-essere umano ai fini dell'attribuzione della responsabilità alla *corporation*. Sul punto, per considerazioni più distese, cfr. Sabia R. (2020), *op. cit.;* v. anche Mazzacuva F., "The Impact of AI on Corporate Criminal Liability: Algorithmic Misconduct in the Prism of Derivative and Holistic Theories", in *Revue Internationale de Droit Pénal*, 2021, 1, p. 143 ss., nonché, con specifico riferimento all'ordinamento statunitense, Diamantis M.E. (2019), *op. cit.* In termini generali sui caratteri della responsabilità vicariale e della identificazione, Gobert J., Punch M., *Rethinking Corporate Crime*, Cambridge, Cambridge University Press, 2003, p. 55 ss.

[59] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (*Regolamento sull'intelligenza artificiale*), di seguito indicato nel testo come *AI Act.*

[60] *AI Act*, considerando 26.

[61] *AI Act*, art. 3, n. 4. Il Regolamento si applica ai *deployer* che hanno il loro luogo di stabilimento o sono situati nell'UE, ma anche in un paese terzo, laddove l'output prodotto dal sistema di IA sia utilizzato nell'Unione (cfr. *AI Act*, art. 2, comma 1, lett. *b* e *c*).

[62] Si prevedono poi specifiche regole per i sistemi di IA con finalità generali nel Capo V dell'*AI Act* (artt. 51 ss.). Sono fuori dal campo di applicazione del Regolamento i sistemi che presentano rischi minimi o assenti, permessi dunque senza restrizioni, anche se l'*AI Act* promuove l'adozione di codici di condotta volontari.

rischio[63] – la cui individuazione è finalizzata ad assicurare un livello costante ed elevato di tutela degli interessi pubblici in materia di salute, sicurezza e diritti fondamentali[64].

Lasciando in questa sede da parte i casi di imprese qualificate come produttori, fornitori etc. di sistemi di IA – ma sottolineando comunque che l'inquadramento non è rigido, prevedendosi casi di possibile 'riqualificazione'[65], da cui discendono obblighi differenziati in base alle varie categorie –, nella prospettiva di interesse occorre soffermarsi sulle ricadute della normativa sulle *corporation* che si limitino a utilizzare professionalmente l'IA nelle proprie attività. Ipotizziamo si tratti di un ente che impieghi un sistema di IA per la creazione e gestione di documenti, o per lo *screening* delle transazioni per la prevenzione del rischio frode o riciclaggio, o per l'*onboarding* e il monitoraggio della clientela nell'ambito delle procedure *know-your-customer*: per tali *deployer*, il Regolamento imporrà anzitutto di inventariare i sistemi in concreto impiegati (o che si programma di impiegare) e inquadrarli alla luce della predetta classificazione.

Il *deployer* è, invero, una figura centrale se, come si legge nei considerando del Regolamento, molti rischi legati a tali sistemi derivano proprio dal modo in cui essi sono utilizzati; costui è nella posizione migliore per individuare potenziali rischi significativi non previsti nella fase di sviluppo, in ragione di una conoscenza più puntuale del contesto di utilizzo e delle persone o gruppi che potrebbero essere interessati[66].

Ciò posto, da una lettura dell'Allegato III, dedicato ai sistemi ad alto rischio, si comprende come diverse delle tecnologie in uso nelle aziende potranno potenzialmente rientrare in tale novero[67]. Non si può al riguardo generalizzare, essendo indispensabile un *impact assessment*

---

[63] *AI Act*, art. 6, comma 1, nonché l'elenco di cui all'Allegato III, che ricomprende sistemi di IA nei seguenti settori: biometria, infrastrutture critiche, istruzione, occupazione, accesso ai servizi essenziali, sia pubblici che privati, attività di contrasto, immigrazione, amministrazione della giustizia e processi democratici.

[64] Cfr. *AI Act*, considerando 7.

[65] La distinzione tra fornitore e *deployer* è tutt'altro che netta, e il *deployer* potrebbe rischiare di essere riqualificato come fornitore in determinati scenari, il che farà scattare ulteriori obblighi. L'*AI Act* contempla infatti espressamente casi (art. 25, comma 1) in cui qualsiasi distributore, importatore, *deployer* o altro terzo sia da considerarsi fornitore di un sistema di IA ad alto rischio (se appone il proprio nome o marchio su un tale sistema già immesso sul mercato o messo in servizio; se vi apporta una modifica sostanziale; se modifica la finalità prevista di un simile sistema di IA che non è stato classificato come ad alto rischio in modo tale che diventi un sistema ad alto rischio).

[66] Lo sottolinea Pietrocarlo E., "La *predictive policing* nel Regolamento europeo sull'intelligenza artificiale", in *La Legislazione penale web*, 26 settembre 2024, p. 26, richiamando il considerando 93.

[67] Già Nisco A. (2022), *op. cit.*, notava come la materia della *compliance* digitale andrebbe verosimilmente ricondotta alla categoria dei sistemi di IA ad alto rischio, al tempo riferendosi alla proposta di Regolamento europeo.

sulle caratteristiche del singolo sistema; ma, ad esempio, le prime analisi segnalano che tali sono i sistemi di IA utilizzati per il *credit scoring* dagli istituti di credito; quelli per la selezione, il monitoraggio e la valutazione dei dipendenti; quelli per la profilazione degli individui[68].

Il Regolamento stesso fissa, peraltro, delle eccezioni, che a loro volta complicano il quadro di riferimento per gli operatori: non sarà considerato ad alto rischio un sistema di IA di cui all'Allegato III ove non presenti un rischio significativo di danni per la salute, la sicurezza, i diritti fondamentali etc., e quindi ad esempio ove sia utilizzato per eseguire un compito procedurale limitato, o sia destinato a rilevare schemi decisionali/deviazioni da precedenti schemi decisionali e non sia finalizzato a sostituire o influenzare la valutazione umana precedentemente completata senza un'adeguata revisione umana; mentre la già citata profilazione di persone fisiche sarà da ritenersi sempre ad alto rischio[69].

Quanto agli obblighi in capo ai *deployer* dei sistemi di IA ad alto rischio, essi sono tratteggiati all'art. 26 del Regolamento, e ci sembra si possano ricondurre a quattro macro-categorie[70]: *i)* gestione del rischio, mediante l'adozione di idonee misure tecniche e organizzative a garanzia dell'utilizzo dei sistemi, conformemente alle istruzioni per l'uso che accompagnano tali sistemi; *ii)* sorveglianza umana, affidata a persone fisiche che dispongono della competenza, della formazione e dell'autorità necessarie nonché del sostegno necessario; *iii)* monitoraggio e *reporting* con riferimento al funzionamento del sistema di IA ad alto rischio, prevedendosi che il *deployer* sia anche tenuto a informare, a seconda dei casi, il fornitore, distributore, la pertinente autorità di vigilanza del mercato etc. nelle circostanze in cui ravvisi un rischio per la salute, la sicurezza o i diritti fondamentali delle persone, nonché ove si verifichi un incidente grave; *iv)* trasparenza, informazione e documentazione, richiedendosi la conservazione per un certo tempo dei *log* generati automaticamente dal sistema di IA ad alto rischio; in caso di messa in servizio o uso sul luogo di lavoro, una informativa *ex-ante* ai lavoratori interessati e ai loro rappresentanti, da parte del *deployer*-datore; nonché, nel caso di sistemi di IA ad alto rischio che adottano (o assistono nell'adozione di) decisioni che riguardano persone fisiche, una informativa a queste ultime.

---

[68] A&O Shearman, "Zooming in on AI – #4: What is the interplay between "Deployers" and "Providers" in the EU AI Act?", 16 settembre 2024, https://www.aoshearman.com/en/insights/ao-shearman-on-tech/zooming-in-on-ai-4-what-is-the-interplay-between-deployers-and-providers-in-the-eu-ai-act#6.

[69] *AI Act*, art. 6, comma 3.

[70] Obblighi aggiuntivi relativi a una valutazione d'impatto sui diritti fondamentali, ai sensi dell'art. 27, incombono, oltre che su soggetti pubblici, su enti privati che forniscono servizi pubblici o che impiegano taluni sistemi ad alto rischio nel contesto creditizio o assicurativo: cfr. *AI Act,* Allegato III, punto 5, lettere b) e c).

Si stabiliscono, poi, anche obblighi di cooperazione con le autorità competenti "in merito a qualsiasi azione intrapresa da dette autorità in relazione al sistema di IA ad alto rischio" (art. 26, comma 12). E v'è forse da chiedersi quali possano essere per l'ente i risvolti di una simile cooperazione se, ad esempio, nel mettere assieme le informazioni per il *reporting*, o in sede di indagini interne a fronte di un grave incidente in ipotesi culminato in un reato presupposto, emergano lacune di carattere organizzativo che possano radicare la responsabilità *ex* D.Lgs. n. 231/2001[71].

L'insieme di tali obblighi, infine, risulta presidiato, in rapporto al tipo di violazione, da significative sanzioni amministrative pecuniarie per la non conformità, che per l'impresa sono parametrate al fatturato[72].

Insomma, sebbene la *timeline* di implementazione del Regolamento si snodi su orizzonti di lungo periodo e nella consapevolezza che occorrerà anche guardare alle soluzioni che verranno adottate dagli stati membri, una simile congerie di disposizioni è destinata a inaugurare un nuovo, ampio capitolo della *corporate compliance* aziendale, in punto di identificazione dei rischi, adozione di appropriate misure di contenimento, istituzione di funzioni con apposita *expertise* IA, valutazione di interferenze con altre normative, spingendo sempre più verso una analisi a carattere integrato.

Un *leitmotiv* della legislazione europea, quello della responsabilizzazione dell'impresa anche attraverso la previsione di obblighi di *compliance* presidiati da sanzioni, che negli ultimi anni abbiamo imparato a conoscere nei diversi ambiti – protezione dei dati, *cybersecurity*, servizi digitali, *due diligence* di sostenibilità, etc.

L'approccio della regolamentazione dell'IA si caratterizza, però, per la scelta di non puntare sulla *co-regulation* pubblico-privato (*i.e.* valorizzare la prospettiva dell'*accountability*, come fatto, ad esempio, nel GDPR), preferendo una disciplina rigida, dove è il legislatore che stabilisce quali sono i sistemi ad alto rischio e quali sono gli obblighi. Colgono nel segno le osservazioni di chi vede qui una criticità, legata al fatto che risulterà difficile modulare le misure da adottare in base alle caratteristiche dell'impresa, anche perché gli obblighi sono sostanzialmente i medesimi – senza reali differenze per *industry* o dimensione[73] – per tutti gli operatori appartenenti a una data categoria. La prospettiva è quella di ritrovarsi a inseguire la rapida evoluzione

[71] Sul punto, v. le considerazioni di Mangione A., *Intelligenza artificiale, attività d'impresa e diritto penale. La funzione di garanzia nell'organizzazione e dell'organizzazione per la sorveglianza dell'AI*, Torino, Giappichelli, 2024, p. 389 s., il quale, osservando che le informazioni da comunicare all'autorità potrebbero contenere elementi *contra reum*, o sviluppi in tale direzione, paventa una possibile lesione dei diritti di difesa e la violazione del principio *nemo tenetur se detegere*.

[72] Cfr. *AI Act*, art. 99.

[73] Finocchiaro G., *Intelligenza artificiale: Quali regole?*, Bologna, Il Mulino, 2024, p. 120 ss.

tecnologica dovendo aggiornare continuamente la valutazione dei rischi già a livello di normativa.

È invece da condividere, su questo terreno, l'idea, come è stato detto efficacemente, che non solo l'organizzazione debba avvalersi delle nuove tecnologie, ma che anche la tecnologia debba avvalersi delle organizzazioni[74], nel senso di introiettare modelli di gestione del rischio *tailor-made*, alla cui conformazione contribuiscano anche i destinatari dei precetti.

4. Uno sguardo all'esperienza comparata: i recenti sviluppi del Department of Justice statunitense

La portata dell'impatto sulla *compliance* penale delle nuove tecnologie, e in specie dell'IA, non è argomento che interessa solo il regolatore europeo. In tempi recentissimi, una importante conferma giunge anche dall'esperienza degli Stati Uniti, storicamente la 'culla' della *corporate criminal liability* [75] e, in tempi più recenti, dei *compliance program*.

Il riferimento è all'ultimo aggiornamento (settembre 2024), del documento della Criminal Division del Department of Justice (DoJ) utilizzato dai *prosecutor* federali per valutare l'efficacia dei *compliance program* aziendali. Si tratta dell'*Evaluation of Corporate Compliance Programs* – ECCP[76], una vera e propria *roadmap* che include le domande prese in considerazione dai pubblici ministeri per valutare, anche in vista delle decisioni da assumere in merito alle indagini – il riferimento è alla scelta se procedere con l'esercizio dell'azione penale, o intraprendere le possibili strade alternative ben conosciute alla prassi giudiziaria nordamericana[77] – l'adeguatezza del *compliance* program.

---

[74] Nisco A. (2022), *op. cit.*

[75] Per uno sguardo d'insieme sul modello di *corporate criminal liability* statunitense, Arlen J., Kraakman R.H., "Controlling Corporate Misconduct: An Analysis of Corporate Liability Regimes", in *New York University Law Review*, 1997, 72(4), p. 687 ss.; Laufer W.S., *Corporate Bodies and Guilty Minds. The Failure of Corporate Criminal Liability*, Chicago, University of Chicago Press, 2006. Nella letteratura italiana, a livello monografico, cfr. De Maglie C., *L'etica e il mercato. La responsabilità penale delle società*, Milano, Giuffré, 2002, p. 12 ss.; Sabia R. (2022), *op. cit.;* Colacurci M., *L'illecito "riparato" dell'ente. Uno studio sulle funzioni della* compliance *penalistica nel D.Lgs. n. 231/2001*, Torino, Giappichelli, 2022, p. 135 ss.

[76] U.S. Department of Justice, Criminal Division, *"Evaluation of Corporate Compliance Programs"*, versione aggiornata a settembre 2024, consultabile all'indirizzo https://www.justice.gov/criminal/criminal-fraud/page/file/937501/dl.

[77] Tra i molti lavori sul tema della dottrina nordamericana, si veda Orland L., "The Transformation of Corporate Criminal Law", in *Brooklyn Journal of Corporate Financial & Commercial Law*, 2006, 1, p. 45 ss.; Uhlmann D.M., "Deferred Prosecution and Non-Prosecution Agreements and the Erosion of Corporate Criminal Liability", in *Maryland Law Review*, 2013, 72, p. 1295 ss.; Garrett B.L., *Too Big To Jail: How Prosecutors Compromise with Corporations*, Cambridge (Mass.), Harvard University Press, 2014; Alexander C.R., Cohen M.A., "The Evolution of Corporate Criminal Settlements: An Empirical Perspective on Non-Prosecution, Deferred Prosecution, and Plea Agreements", in *American Criminal Law Review*, 2015, 52, p. 537 ss.

Prima di esaminare da vicino le novità introdotte, vale la pena ricordare la genesi dell'ECCP, che nasce nel 2017 ed è stato già aggiornato a più riprese[78]. L'ECCP va letto in 'combinato disposto' con le prescrizioni contenute nei *Principles of Federal Prosecution of Business Organizations* (attualmente nel *Justice Manual*) e, a livello settoriale, nella *FCPA Resource Guidance*. Questo set di *guideline*, come si sa, si propone l'obiettivo di 'standardizzare' e 'strutturare' la discrezionalità dei *prosecutor*[79].

L'ECCP, in particolare, si focalizza su tre interrogativi chiave, per cui i pubblici ministeri debbono verificare se: 1) il *compliance program* è ben concepito; 2) è dotato di risorse e poteri adeguati per operare efficacemente; 3) funziona nella pratica. Si elabora, dunque, una sorta di *checklist*, che, per ciascuna area tematica individuata, guida il *prosecutor* nell'analisi dell'efficacia del *compliance program*[80], con riferimento a specifici punti di attenzione ma adottando, al contempo, un approccio flessibile e individualizzato, che permetta di valorizzare anche altri fattori che possono avere un impatto sulle misure di *compliance* (tra cui, ma non solo, le dimensioni e il settore operativo dell'impresa, l'estensione geografica, il contesto normativo di riferimento, etc.).

È possibile astrarre alcuni principi di fondo che dovrebbero informare le attività di valutazione poste in essere: accertare se il *compliance program* sia 'ritagliato' sulle specificità dell'organizzazione; constatare la revisione e aggiornamento delle procedure *in action* in aggiunta al preliminare *risk assessment*; dissociare la verifica sulla qualità della *compliance* dal fatto che si sia verificato il reato, rifuggendo la logica del senno di poi; prevedere risorse adeguate, considerato il rilievo del patrimonio informativo della *corporation* per mantenere un sistema di *compliance* efficace.

Già nelle precedenti versioni dell'ECCP si evidenziava, altresì, la centralità dell'accesso ai dati per il monitoraggio della *compliance* e la possibilità di testare *policy*, controlli e transazioni, così che l'ente fosse messo in condizione di fronteggiare i rischi in evoluzione. Proprio in tale ottica – anche in linea con l'idea di far tesoro delle *lesson learned* sia sul versante dell'accusa, sia su quello delle *corporation* – si colloca l'aggiornamento da ultimo apportato, volto a incorporare nell'ECCP la valutazione dei rischi posti dalle nuove tecnologie, compresa l'IA.

---

[78] Dopo un primo aggiornamento nel 2020, nel marzo 2023 l'ECCP è stato nuovamente rivisto per considerare, tra l'altro, come i *compliance program* affrontino l'uso di dispositivi personali (es. cellulari) e piattaforme di comunicazione, chiarendo che i *prosecutor* ricercheranno più attivamente i dati delle applicazioni di messaggistica di terze parti e che la mancata conservazione e produzione di tali dati potrà influire negativamente sulle prospettive di *resolution*.

[79] In argomento v. Lafave W.R., "The Prosecutor's Discretion in the United States", in *American Journal of Comparative Law*, 1970, 18, p. 532 ss.

[80] Per alcune considerazioni su tali *guideline*, Gullo A. (2020), *op. cit.*

Già lo scorso marzo, il Deputy Attorney General Monaco aveva pubblicamente annunciato l'imminente nuova revisione del documento, confermata poi a settembre in occasione di una conferenza annuale organizzata dalla Society of Corporate Compliance and Ethics[81]. In termini generali, l'aggiornamento del documento tocca tre aree principali: la già menzionata valutazione e gestione dei rischi legati alle nuove tecnologie, come l'IA; il ruolo, ulteriormente enfatizzato, dell'analisi dei dati; la protezione dei *whistleblower*.

Soffermando qui l'attenzione sul primo ambito, l'aggiornamento dell'ECCP attesta come il DoJ si attenderà, d'ora in avanti, che le imprese mettano appunto in campo controlli e misure adeguati a mitigare i rischi associati all'uso dell'IA[82].

L'*update* inserisce nel documento, nella sezione relativa al primo dei quesiti sopra ricordati (il *compliance program* è ben concepito?) e nella parte riguardante il *risk assessment*, alcune specifiche domande[83] che i *prosecutor* dovranno considerare nel contesto della gestione dei rischi emergenti da parte della *corporation*, e che paiono ruotare attorno a un triplice ordine di valutazioni, ossia:

- se l'impresa effettui un *assessment* dei rischi emergenti, interni ed esterni, tra cui l'IA, rispetto alla capacità dell'ente di rispettare la legge, anche penale; si richiama l'inclusione o meno dei rischi in oggetto in più ampie strategie di gestione (*enterprise risk management* – ERM) e di *governance*;
- se l'ente stia ponendo in essere misure per mitigare le conseguenze negative indesiderate dell'IA nelle attività di *business* e nel *compliance program*, e l'uso improprio di tali tecnologie; se abbia implementato controlli sull'attendibilità, l'affidabilità e l'uso conforme alla legge dell'IA, ove la impieghi, ancora, sia per finalità commerciali sia per attività di *compliance*;
- se si valorizzi adeguatamente il fattore umano, sia in relazione alla base decisionale utilizzata per valutare l'IA, sia in relazione alle responsabilità sull'uso della medesima e alla formazione dei dipendenti sulle tecnologie emergenti.

---

[81] È possibile leggere il testo dell'intervento della Principal Deputy Assistant Attorney General Argentieri al seguente indirizzo: https://www.justice.gov/opa/speech/principal-deputy-assistant-attorney-general-nicole-m-argentieri-delivers-remarks-society.

[82] Benjet B.H., Jurtz J., "The Evolution of DOJ and SEC Expectations for Corporate Compliance Programs and Staying Ahead of the Curve", in *Villanova Law Review*, 2021, p. 945, evidenziavano – già prima del recente *update* dell'ECCP – che la disponibilità sul mercato di strumenti per assistere le *corporation* nella gestione dei *Big Data* e di tecnologie basate sull'IA possono sia incoraggiare una cultura della *compliance*, fornendo la base conoscitiva per implementare un *compliance program* sempre più efficace, sia, proprio per questo, elevare gli standard di conformità attesi da parte delle agenzie di *enforcement*.

[83] U.S. Department of Justice, Criminal Division (2024), *op. cit.*

L'impiego dell'IA è poi espressamente menzionato anche nella diversa sezione del documento che attiene al corretto funzionamento del *compliance program* (funziona nella pratica?), nella parte che illustra il miglioramento e le revisioni dello stesso[84]. In particolare, quanto agli aggiornamenti, l'ECCP evidenzia l'importanza di domandarsi se la *corporation* che impieghi l'IA nelle proprie attività stia monitorando e testando tali tecnologie per valutarne funzionamento e conformità a codici di condotta e *policy* aziendali, e quanto velocemente sia in grado di intervenire per correggere le decisioni prese dall'IA.

Quali le conseguenze principali di tali innovazioni? Le prime analisi d'impatto[85] evidenziano importanti cambiamenti nelle verifiche che le imprese saranno chiamate a svolgere. L'ECCP è, invero, non solo un documento di orientamento per le valutazioni dei pubblici ministeri sull'idoneità dei *compliance program*, ma anche un riferimento centrale per le *corporation* nella progettazione della propria architettura di prevenzione.

In primo luogo, la stessa definizione di IA adottata nelle *guideline* è ampia[86], e imporrà quindi agli enti di considerare attentamente se le soluzioni tecniche da esse implementate possano rientrare nell'ambito di applicazione dell'ECCP.

Le novità introdotte evidenziano, poi, la necessità di adottare un approccio basato sul rischio e sulla trasparenza e *accountability*. Infatti, la natura di *black box* di alcuni sistemi di IA non può, secondo l'ECCP, rappresentare una giustificazione: le imprese devono garantire, in particolare, che qualsiasi *compliance program* che si avvalga dell'IA contempli *due diligence* e *procurement standard* efficaci per i modelli o strumenti di terze parti utilizzati, esperti interni con competenze tecniche, l'uso dei dati da parte della *funzione compliance* per individuare i rischi e avere consapevolezza del funzionamento pratico delle nuove tecnologie e del loro impatto.

Consegue che l'evoluzione delle nuove tecnologie imporrà alle aziende un continuo monitoraggio – specie con riferimento alla valutazione dell'efficacia del *compliance program* (es. sul versante del rilevamento automatico del rischio e del *real time monitoring*, per i casi d'uso ad alto rischio) e la pronta attivazione per correggere i problemi riscon-

[84] U.S. Department of Justice, Criminal Division *(2024), op. cit.*

[85] Cfr. Gibson Dunn, "DOJ Updates Its Evaluation of Corporate Compliance Programs Guidance Focused on AI and Emerging Technologies", 30 settembre 2024, https://www.gibsondunn.com/doj-updates-evaluation-of-corporate-compliance-programs-guidance-focused-on-ai-and-emerging-technologies/.

[86] Si segue la definizione prevista nel memo dell'Office of Management and Budget del marzo 2024: U.S. Department of Justice, Criminal Division (2024), *op. cit.*

trati, o le decisioni assunte mediante l'IA, ove non siano rispettati gli standard di conformità[87].

Va detto, per completezza di visuale rispetto alle novità introdotte, che l'ECCP ora contempla anche nuovi criteri relativi all'uso e all'analisi dei dati da parte delle imprese[88]. Le domande[89] che i *prosecutor* – e, come detto, le imprese – sono chiamati a porsi riguardano in tal senso la circostanza che il personale addetto alla *compliance* abbia modo di accedere alle fonti rilevanti in modo tempestivo, e che la *corporation* sfrutti adeguatamente le risorse di *Big Data analytics* per rendere le operazioni di *compliance* più efficienti, assicurando anche la qualità dei dati.

Le linee guida del DoJ, nella versione aggiornata, ci sembra quindi si pongano 'in scia' con molte delle indicazioni già positivizzate, in Europa, dall'*AI Act*. Le domande sulla base delle quali i *prosecutor* statunitensi passeranno al vaglio i *compliance program* d'ora in avanti attribuiscono rilievo alle tecnologie nel contesto aziendale da una prospettiva ambivalente: da una parte, il DoJ sottolinea i rischi, evocando la possibilità di radicare un giudizio negativo circa l'efficacia del *compliance program* nell'assente, o insufficiente, strategia di gestione e supervisione sull'utilizzo di tali algoritmi; dall'altro, il Dipartimento invita gli enti a prevedere risorse adeguate per l'adozione nelle attività di *compliance* di sistemi di *data analytics*.

Un approccio realista, che evidenzia, assieme alla consapevolezza circa i pericoli legati a un uso pervasivo e *unsupervised* dell'automazione, una analoga consapevolezza rispetto all'importanza – e forse, a fronte dell'inarrestabile evoluzione tecnologica, all'irrinunciabilità – di valorizzarne, e guidarne, l'impiego a beneficio della *compliance* aziendale.

---

[87] Le organizzazioni dovranno adattare i sistemi di *compliance* alla rapida evoluzione degli standard legali e tecnici relativi all'IA. Si rileva nelle *guideline* del DoJ che esistono già delle *guidance*, anche da parte delle agenzie federali, sulle migliori pratiche di *governance* e conformità dell'IA, destinate però in gran parte a un uso volontario (es. l'*AI Risk Management Framework* pubblicato dal National Institute of Standards and Technology – NIST): cfr. U.S. Department of Justice, Criminal Division (2024), *op. cit.*

[88] U.S. Department of Justice, Criminal Division (2024), *op. cit.*

[89] U.S. Department of Justice, Criminal Division (2024), *op. cit.*

Rivista di Politica Economica

La Rivista di Politica Economica è stata fondata nel 1911 come "Rivista delle società commerciali" ed ha assunto la sua attuale denominazione nel 1921. È una delle più antiche pubblicazioni economiche italiane ed ha sempre accolto analisi e ricerche di studiosi appartenenti a diverse scuole di pensiero. Nel 2019 la Rivista viene rilanciata, con periodicità semestrale, in un nuovo formato e con una nuova finalità: intende infatti svolgere una funzione diversa da quella delle numerose riviste accademiche a cui accedono molti ricercatori italiani, scritte prevalentemente in inglese, tornando alla sua funzione originaria che è quella di discutere di questioni di politica economica, sempre con rigore scientifico. Gli scritti sono infatti in italiano, più brevi di un paper accademico, e usano un linguaggio comprensibile anche ai non addetti ai lavori. Ogni numero è una monografia su un tema scelto grazie ad un continuo confronto fra l'editore e l'*Advisory Board*. La Rivista è accessibile online sul sito di Confindustria.

Redazione Rivista di Politica Economica
Viale Pasteur, 6 – 00144 Roma (Italia)
e-mail: rpe@confindustria.it
https://www.confindustria.it/home/centro-studi/rivista-di-politica-economica

Direttore responsabile
Silvia Tartamella

Coordinamento editoriale ed editing
Paola Centi
Adriana Leo

Edito da:

CONFINDUSTRIA SERVIZI

Confindustria Servizi S.p.A.
Viale Pasteur, 6 - 00144 Roma