L'ANTICORRUZIONE AL BIVIO DELL'ALTERNATIVA DIGITALE

Ilaria Antonella Esposito*

SOMMARIO: 1.- Anticorruzione e transizione digitale: lo stato dell'arte; 2.- Nuove tecnologie e prevenzione della corruzione nelle pubbliche amministrazioni: dalla "mera" digitalizzazione a potenziali nuovi impieghi?; 3.- La prevenzione della corruzione quale idealtipo applicativo della c.d. "digital criminal compliance" nel settore privato; 4.- (In)esistenza di un punto di equilibrio: prospettive attuali e future dell'anticorruzione automatizzata tra sfera pubblica e privata.

1.- **Anticorruzione e transizione digitale: lo stato dell'arte.**

In tempi di cambiamenti globali più o meno intesi, incidenti in vario modo sul piano economico, sociale e anche giuridico, l'anticorruzione rappresenta un trasversale presidio di legalità dal quale non può prescindersi.

Senza la pretesa di un'indagine sociologica, può nondimeno affermarsi che processi epocali, quali le transizioni gemelle (verde e digitale), implichino un inevitabile adattamento del fenomeno corruttivo, tanto nelle sue concrete manifestazioni quanto nelle strategie di repressione e prevenzione.

È in quest'ultima prospettiva che può cogliersi, invero, la risaputa attitudine camaleontica della corruzione, la cui sperimentata resilienza alle evoluzioni influenza le contromisure messe in campo dal suo (atecnico) *contrarius actus* – l'anticorruzione –, giustificandone il continuo aggiornamento.

Emblematiche conferme, in questo senso, possono scorgersi sia nelle sempre più avvertite esigenze di contrasto, a fronte dell'avanzare di sofisticati schemi corruttivi[1], talvolta frutto del cambiamento[2], sia nell'auspicato efficientamento delle misure di prevenzione, che proprio nel flusso dei menzionati processi innovativi scorgono un'indubbia "chance" di affinamento.

Tralasciando la componente "green", sulla quale continuano a pendere chiamate all'integrazione con le politiche anticorruzione[3], è nel rapporto tra queste ultime e la transizione digitale che l'urgenza di tale duplice adattamento (repressivo e preventivo) appare irrimandabile. Non fosse altro perché, al contrario della transizione verde, quella digitale[4] si presta all'ossimorica conformazione di potenziale fattore d'innesco e promettente inibitore dei fenomeni *lato sensu* corruttivi.

Ciò, a ben vedere, nella misura in cui le nuove tecnologie si pongano, allo stesso tempo, come fonte inedita e (non) testato palliativo di problemi sistemici – qual è la corruzione – spesso (se non sempre)

---

* Dottoranda di ricerca in diritto penale presso l'Università degli Studi della Campania "Luigi Vanvitelli".

[1] Ad esempio, sul fenomeno della c.d. "fiscal corruption", si veda A. Gullo, *Exploring the Interconnections Between Tax Crime and Corruption: National Report for Italy*, in *VAT fraud, Interdisciplinary Research on Tax crimes in the EU – VIRTEU*, Coventry University 2022.

[2] Ci si riferisce, in particolare, alla piaga corruttiva dell'economia verde, ove l'illecita erogazione dei certificati energetici ne rappresenta il dato più allarmante, e alle connessioni tra criptovalute e corruzione; in proposito, si veda rispettivamente il rapporto di Transparency International Italia dal titolo *Corruzione e frode nella green economy,* 2013 e S. Elsayed, *Cryptocurrencies, corruption and organised crime*, *Transparency International Anti-Corruption Helpdesk Answer*, 2023.

[3] Sul punto, v. F. Merenda, *L'anticorruzione tra l'integrazione con le altre politiche e la prospettiva della nuova Direttiva europea*, in *Federalismi.it* 1 (2025) 63ss. o, più in generale, E. Carloni, *L'anticorruzione. Politiche, regole, modelli*, Bologna 2023, 270ss.

[4] Sul tema si veda L. Picotti, *Diritto penale, tecnologie ed intelligenza artificiale: una visione d'insieme*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (curr.), *Cybercrime*, Milano 2023, 32ss., Id., *New Technologies as Tools for and Means Against Crime: Substantial Aspects*, in *Revue Internationale de Droit Pénal* 2 (2020) 183.

esposti a "deficit" d'efficienza nelle strategie di contrasto[5], e che quindi più di altri si candidano a promettenti tentativi d'innesto della intelligenza artificiale (d'ora in avanti IA).
È divenuto, infatti, pressoché inconscio il pensiero per cui gli algoritmi facciano meglio – e in tempi minori – quanto di decisionale ed analitico spetta(va) alle capacità umane[6], almeno là dove il substrato conoscitivo sia rappresentato da grandi moli di dati oggettivi da catalogare e/o classificare.
Finché l'automazione si limiti ad incidere sulla quantità dei dati a disposizione, razionalizzandoli in funzione di una variabile (es. flussi di denaro anomali)[7], ben poco potrebbe in astratto essere opposto all'utilizzo di tali tecnologie nell'arsenale degli strumenti di prevenzione della corruzione, trattandosi all'evidenza di un chiaro esempio di "artificial intelligence for good".
Si discute, del resto, di una strada già parzialmente intrapresa dal legislatore del 2023 il quale, nell'introdurre il nuovo Codice degli appalti pubblici (D.Lgs. 36/2023), ha previsto il potenziamento della Banca dati nazionale dei contratti pubblici, a coronamento dell'integrale approvvigionamento digitale quale dichiarato obiettivo del Piano Nazionale di Ripresa e Resilienza (PNRR)[8].
Di qui, è possibile affermare che la nuova frontiera dell'anticorruzione, rappresentata dalla sfida digitale nelle pubbliche amministrazioni, abbia quantomeno inaugurato il suo corso.
Invero, al di là di caute prese di posizione e report informativi da parte delle organizzazioni di categoria[9], oltre che di varie sperimentazioni avviate in ordinamenti diversi dal nostro[10], sarebbe più corretto registrare, allo stato attuale, anzitutto un processo di digitalizzazione, come quello completato nel settore degli appalti pubblici, e solo a latere primissime applicazioni delle potenzialità dell'IA, in specie nel settore privato[11].
Peraltro, l'attuale rapporto tra anticorruzione e transizione digitale se certo non può essere letto in termini definitivi, in quanto il connubio è tuttora in corso, deve nondimeno transitare attraverso lo scrutino di due lenti – amministrativista e penalistica – su cui grava altresì il peso della più recente tendenza legislativa alla creazione di una sorta di zona grigia tra le due leve[12]. Zona grigia che, a dire

[5] Per una più ampia visione sulle diverse stagioni dei delitti di corruzione in Italia, cfr. *ex multis*, V. Mongillo, *La legge "Spazzacorrotti": ultimo approdo del diritto penale emergenziale nel cantiere permanente dell'anticorruzione*, in *Diritto penale contemporaneo* 5 (2019) 231ss.; P. Severino, *La nuova legge anticorruzione*, in *Diritto penale contemporaneo* (2013) 7ss.; G. Balbi, *I delitti di corruzione. Un'indagine strutturale e sistematica*, Napoli 2003; T. Padovani, *Il problema "Tangentopoli" tra normalità dell'emergenza ed emergenza della normalità*, in *Rivista italiana di diritto e procedura penale* (1996) 448ss.
[6] C. Burchard, *L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società*, in *Rivista Italiana di Diritto e Procedura Penale* 4 (2019) 1924.
[7] Sul tema, si veda P. Severino, *Intelligenza artificiale e diritto penale*, in U. Ruffolo (cur.), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Torino 2020, 537 nella parte in cui afferma che «l'implementazione di siffatti sistemi è legata infatti all'esigenza, chiaramente avvertita sia nell'ambito delle organizzazioni pubbliche e private, sia nel settore del "law enforcement", di sfruttare appieno il potenziale offerto dai c.d. "big data" e, dunque, di gestire e analizzare un'enorme quantità di informazioni attraverso metodi più sofisticati di quelli tradizionali».
[8] Nello specifico, si tratta della "milestone" M1C1-75.
[9] Si vedano i "working papers" rispettivamente dell'OCSE, *Generative AI for Anti-Corruption and integrity in government* 1 (2024) e di Transparency International, *The corruption risks of artificial intelligence* (2022).
[10] F. De Simone, *L'implementazione delle nuove tecnologie nelle politiche anticorruzione*, in G. Balbi, F. De Simone, A. Esposito, S. Manacorda (curr.), *Diritto penale e intelligenza artificiale. "Nuovi scenari"*, Torino 2022, 60ss., la quale riporta i casi del sistema cinese Zero Trust e delle c.d. mappe autorganizzanti elaborate dai ricercatori dell'Università di Valladolid (Spagna). Di queste ultime ne fa menzione anche l'intervento di A.R. Castaldo, *New perspectives of fighting corruption through AI*, in *Iura and Legal Systems* 1 (2022) 2 tenuto in occasione del Quinto Simposio Internazionale sull'Anticorruzione, 4-5 novembre 2021, Cina.
[11] V. *infra*, par. 3.
[12] Il riferimento è chiaramente all'abrogazione del reato di abuso d'ufficio, compiuta con la legge Nordio (n. 114/2024); in proposito, utilizza l'espressione della "zona grigia" E. Carloni, *L'abuso di potere, tra contrasto penale e contrasto amministrativo: i limiti dell'anticorruzione amministrativa*, in *Rivista Italiana di Diritto e Procedura Penale* 2 (2024) 641ss.

il vero – nel contesto qui in esame – pare comunque assottigliarsi sotto altro profilo: è infatti indubbio che l'utilizzo delle nuove tecnologie rappresenti l'ennesima prova del processo osmotico in atto nella stagione della prevenzione mediante organizzazione tra impianto pubblico e privato[13].
Consolidando i termini dello "scambio" originario, per cui le logiche pianificatrici nel pubblico (con i piani anticorruzione) sono state coniate a partire da quelle già invalse nel settore privato (con i modelli 231), è oggi nuovamente l'apporto fornito dal secondo a fare da traino al primo, fornendo gli impulsi per una possibile metamorfosi[14] della "compliance" anticorruzione.
L'obiettivo del lavoro è quindi quello di mettere in luce i vantaggi e i rischi dell'automazione nel settore *de quo*, che infine dovrà fare i conti con l'incertezza dell'attuale quadro normativo sospeso tra una regolamentazione eurounitaria già parzialmente in vigore – il Regolamento (UE) 2024/1689, noto come Artificial Intelligence Act (AI Act) – e una disciplina nazionale, rimessa dal Regolamento all'autonomia degli Stati membri[15], ancora in fase di approvazione – il d.d.l. 78 del 23/04/2024.
Ci si asterrà, infine, da un esame più accurato della recente proposta di direttiva europea sulla lotta contro la corruzione[16], la quale se da un lato appare confermare l'approccio olistico al fenomeno, fondato sul binomio repressione-prevenzione, dall'altro nulla espressamente prevede circa l'impiego delle tecniche di IA nelle strategie di contrasto.

2.- **Nuove tecnologie e prevenzione della corruzione nelle pubbliche amministrazioni: dalla "mera" digitalizzazione a potenziali nuovi impieghi?**

Dal lato pubblicistico, si è già riferito della presenza del digitale nella recente implementazione del c.d. "e-procurement" e, ad onor del vero, anche nella versione aggiornata dei canali di segnalazione degli illeciti ("whistleblowing")[17].
È la stessa Autorità Nazionale Anticorruzione (ANAC) ad aver d'altronde ammesso – in un suo documento[18] ancorché anteriore alla recente messa a punto delle c.d. banche dati interoperabili[19] – di sfruttare le tecnologie dell'informazione e della comunicazione (note con l'acronimo anglosassone ICT), sottoforma di "open data" aggregati.
Nell'ambito della contrattualistica pubblica, è tuttavia la funzione dei controlli sulle imprese ad aver beneficiato maggiormente dell'avvento del digitale, attesa l'implementazione del c.d. fascicolo

[13] Per una visione d'insieme del fenomeno *de quo*, si vedano A. Gullo, V. Militello, T. Rafaraci, *Il sistema penale di fronte all'interazione pubblico-privato e* hard law-soft law*: profili e questioni*. *Introduzione*, in Id. (curr.), *I nuovi volti del sistema penale fra cooperazione pubblico privato e meccanismi di integrazione fra* hard law *e* soft law, Atti dell'XI corso di formazione interdottorale di diritto e procedura penale "Giuliano Vassalli", Milano 2021 nonché S. Manacorda, *Towards an Anti-Bribery Compliance Model: Methods and Strategies for a "Hybrid Normativity"*, in S. Manacorda, F. Centonze, G. Forti (curr.), *Preventing Corporate Corruption: The Anti-Bribery Compliance Model*, Londra 2014, 3ss.
[14] Si esprime in questi termini E. Birritteri, Big Data Analytics *e* compliance *anticorruzione. Profili problematici delle attuali prassi applicative e scenari futuri*, in *Diritto penale contemporaneo* 2 (2019) 291.
[15] In particolare, l'art. 99 del Regolamento cit. lascia un margine di apprezzamento ai singoli Stati membri circa l'adozione delle misure necessarie, su tutte sanzionatorie, per garantire un'attuazione efficace del Regolamento medesimo.
[16] Per il contenuto del testo, v. https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52023PC0234.
[17] Si tratta di quanto previsto dal D.Lgs. 24/2023 di attuazione della direttiva europea sul "whistleblowing".
[18] Rapporto ANAC-NCPA dal titolo *Using innovative tools and technologies to prevent and detect corruption. Compendium of good practices and practical examples in the use of ICT*, 2021, consultabile al seguente indirizzo https://www.anticorruzione.it/documents/91439/2702092/ANAC+NCPA+Using+innovative+tools+and+technologies+to+prevent+and+detect+corruption.pdf/7bf1e738-9cd2-6ebe-151c-3b0a83ff3ead?t=1640184131127.
[19] Per interoperabilità delle banche dati si intende, ai sensi dell'art. 1 del Capo e Sezione I del CAD, la «caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi». Tale funzione, perno della misura PaDigitale2026 del PNRR, è divenuta inderogabile a partire dal 1° gennaio 2024 e trova applicazione per mezzo dalla Piattaforma Digitale Nazionale Dati (PDND).

virtuale dell'operatore economico (FVOP)[20] che dovrebbe consentire, da un lato, di alleggerire gli oneri istruttori dei privati e, dall'altro, di prevenire episodi di corruzione – da intendersi nella sua più ampia accezione di "maladministration"[21] – attraverso verifiche incrociate sui requisiti richiesti per la partecipazione alle procedure di gara.

Sennonché, malgrado la riferita digitalizzazione del ciclo degli appalti pubblici – certamente da salutare con favore – e il formale[22] abbandono della via cartacea per il "soffio del fischietto", appare doveroso interrogarsi sulle possibilità d'impiego degli strumenti di IA ben oltre l'informativizzazione delle procedure pubbliche, che ad ogni modo – quale forma di sostituzione della macchina al lavoro intellettuale dell'uomo – è classificabile come vero e proprio utilizzo di elaborazione artificialmente indotta[23].

Sotto questo profilo, è ai piani triennali di prevenzione della corruzione a cui occorre guardare.

In altre parole, si tratta di coordinare il presente (il prezioso patrimonio informativo contenuto nelle banche dati in dotazione delle p.a.) con il prossimo futuro (lo sfruttamento di una tale platea di dati al fine di mappare, e meglio contenere, il rischio corruttivo).

Compito non semplice, quest'ultimo, poiché inevitabilmente condizionato della qualità dei dati posti al centro dell'analisi, la cui eventuale inattendibilità è in grado di falsare – e quindi arrestare bruscamente – la valutazione sull'efficacia di quegli strumenti di IA che "vivono" di informazioni eteroindotte. Tanto più se la circolazione di tale patrimonio informativo si inserisca in un contesto più ampio, quale il neo-introdotto Piano integrato di attività e organizzazione (PIAO) nella sua veste di eterogeneo contenitore di moduli organizzativi.

Quanto detto non deve tuttavia scoraggiare. Mai come in questo ultimo biennio (2022-2024), il processo di digitalizzazione delle pubbliche amministrazioni ha fatto passi da gigante[24] gettando le basi per lo step successivo: l'impiego degli algoritmi nell'adozione dei piani anticorruzione. Del resto,

[20] Adottato con delibera ANAC 262 del 20/06/2023, di attuazione dell'articolo 24, c. 4, del D.Lgs. 36/2023. La normativa sui controlli sulle imprese, invece, trova ora spazio nel D.Lgs. 103/2024. Per approfondimenti, si rinvia a B. Ballerini, *La digitalizzazione dei controlli sulle imprese: nuove soluzioni, nuovi problemi?*, in *Federalismi.it* 10 (2024).

[21] È nota la volontà del legislatore del 2012 – con la L.190 – di coniare un concetto di corruzione amministrativa in cui ricomprendere le situazioni in cui «a prescindere dalla rilevanza penale, venga in evidenza un malfunzionamento dell'amministrazione a causa dell'uso a fini privati delle funzioni attribuite» (in tali termini, R. Cantone, *Il sistema della prevenzione della corruzione in Italia*, in *Diritto penale contemporaneo* (2017) 3-4).

[22] In proposito, appare più corretto parlare di formalità in quanto il D.Lgs. 24/2023, pur gerarchizzando i canali di segnalazione degli illeciti, prescrive il ricorso non esclusivo a modalità informatiche basate su sistemi di crittografia; v. diffusamente G. Cossu, L. Valli, *Il* whistleblowing*: dalla Direttiva 1937/2019 al Decreto Legislativo 24/2023*, in *Federalismi.it* 19 (2023) 172ss.

[23] Si riprende un'espressione di E. Lo Monte, *Intelligenza artificiale e diritto penale: una* contradictio in adiecto *per un rapporto problematico*, in *Iura and Legal Systems* 3 (2024) 16 utilizzata per riferirsi, in termini a suo dire meno contradditori, al concetto di IA. Sono invero risapute le difficoltà definitorie, e le speculari obiezioni a cui queste si prestano, che aleggiano attorno alla nozione di "intelligenza" e al suo attributo di "artificiale", v. diffusamente L. Floridi, *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, Milano 2022, 34 laddove ne parla come di «formula scorciatoia». Oggi, tuttavia, l'AI Act ha adottato una definizione di sistema di IA univoca all'art. 3 qualificandolo come «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali».

[24] Precedenti studi, invero, intravedevano proprio nel c.d. "digital gap" il primo scoglio da superare per passare a discutere dell'utilizzabilità degli algoritmi nella costruzione dei piani, cfr. F. Merenda, *Legalità, algoritmi e corruzione: le tecniche di intelligenza artificiale potrebbero essere utilizzate* nel *e* per *il sistema di prevenzione della corruzione?*, in *Rivista Italiana di Informatica e Diritto* 2 (2022) 25; B. Ponti, A. Cerrillo-i-Martínez, F. Di Mascio, *Transparency, digitalization and corruption*, in E. Carloni, M. Gnaldi (curr.), *Understanding and fighting corruption in Europe: From repression to prevention*, Londra 2022, 97ss. e M. Falcone, *La* big data analytics *per conoscere, misurare e prevenire la corruzione*, in M. Gnaldi, B. Ponti (curr.), *Misurare la corruzione oggi. Obiettivi, metodi, esperienze*, Milano 2018, 93.

se non di amministrazione "intelligente"[25], quantomeno di amministrazione digitalizzata è consentito parlare, come minimo riguardo ai segmenti passati in rassegna.

Ciò posto, sembrerebbero sussistere *prima facie* tutte le precondizioni – riassunte nel crescente utilizzo di "big data" retto dal principio di interoperabilità – per tentare di salire al gradino successivo. Se non fosse che, già in prima battuta, diviene logico confrontarsi con un primissimo ostacolo: l'impianto su cui si vuol cercare di innestare l'IA – i piani anticorruzione – sono pur sempre un portato dell'autoregolazione. Ciò vuol dire che, di fianco ad un numero variabile di informazioni ricavabili dall'incrocio tra le banche dati pubbliche, un altrettanto numero a priori indefinibile di dati dev'essere inserito manualmente dal personale a ciò addetto, in virtù della caratteristica propria della "compliance" quale impalcatura costruita "su misura" della singola organizzazione. Di conseguenza, non solo deve prioritariamente investirsi nella formazione dei funzionari, ma gli stessi algoritmi sarebbero confinati ad operare sotto il controllo dell'uomo, attesa l'ineliminabile individualizzazione dei piani che quindi impedirebbe l'elisione dell'"human substratum". Altro è poi il discorso, che si cercherà di affrontare nel prosieguo della trattazione, delle derive "intelligenti" degli algoritmi che potrebbero sviluppare una capacità di autodeterminarsi prescindendo dal controllo umano.

In breve, nel confronto con un altro specifico settore – il reclutamento del personale nelle p.a. – parimenti interessato dall'apporto dell'IA e già al centro di richiami al bilanciamento tra interessi di primario rilievo[26], quello dei piani anticorruzione sembra porsi al riparo dall'utilizzo della forma più invasiva (e problematica) di IA, rappresentata dalle decisioni automatizzate, per almeno due ordini di ragioni: anzitutto perché il Piano triennale di prevenzione della corruzione e trasparenza (PTPCT) è un atto adottato dal Responsabile della prevenzione della corruzione e trasparenza (RPCT) al quale è ricollegato un sistema di responsabilità (dirigenziale, disciplinare ed erariale)[27] che ne presuppone l'esclusiva riferibilità soggettiva; in secondo luogo perché, a valle della fase di mappatura del rischio corruzione, l'adozione delle speculari contromisure preventive non può non passare per la valutazione degli attori a ciò delegati. Insomma, quasi anticipando le istanze di regolazione volte a salvaguardare il dominio umano nei processi automatizzati, la personalizzazione dei piani, che per definizione sottende il rifiuto di qualsivoglia automatismo calato dall'alto[28], appare fungere da "limite naturale" al rischio di indiscriminata trasformazione algoritmica della "compliance" pubblicistica[29].

Fissate queste coordinate, è possibile – se non auspicabile – che gli algoritmi vengano utilizzati a sostegno di talune fasi di costruzione del piano, ad esempio quella di monitoraggio del rischio che più di altre potrebbe trarre benefici dall'automazione. Ed ecco quindi che l'ausilio di strumenti quali la "blockchain" e le "big data analytics" si prospetta di sicuro rendimento[30], trattandosi di tecnologie

[25] Espressione utilizzata da I.M. Delgado, *Automazione, intelligenza artificiale e pubblica amministrazione: vecchie categorie concettuali per nuovi problemi?*, in *Istituzioni del Federalismo* 3 (2019) 645.

[26] Ad es. in tema di procedure di assegnazione delle sedi al personale docente scolastico è nota la sentenza Cons. Stato, Sez. VI, 13/12/2019, n. 8472 che ha affermato il concetto di trasparenza algoritmica nelle decisioni amministrative.

[27] Cfr. L. 190/2012, artt. 1. 12, 13 e 14.

[28] Se è pur vero che i Piani triennali di prevenzione della corruzione e della trasparenza (PTPCT) sono atti derivati "a cascata" dal Piano Nazionale Anticorruzione (PNA), è altrettanto innegabile che i primi si ramificano in autonomia a partire dal secondo, adattandosi al contesto della singola amministrazione. Per un'esaustiva disamina sul tema, nonché per un confronto con i modelli 231, v. R. Bartoli, *I piani e i modelli anticorruzione nei settori pubblico e privato*, in *Diritto penale e processo* 11 (2016) 1507ss.

[29] V. più nel dettaglio *infra*, par. 4.

[30] Recentemente, quello dei benefici derivanti dall'utilizzo di tali tecnologie è stato un tema indagato in letteratura. Tra quella italiana v. Merenda, *Legalità* cit.; M. Letizi, G. Soana, *Le potenzialità del modello di* corporate compliance *integrato basato sulla tecnologia* Blockchain, in *Norme e Tributi Plus – Il sole 24 ore* (2020); Birritteri, *Big Data* cit.; Falcone, *La* big data analytics cit. 90ss.

(le prime) in grado di catalizzare e gestire in registri permanenti le informazioni immesse, rendendole immodificabili e sempre disponibili e di dispositivi (le seconde) capaci di raccogliere, conservare ed elaborare enormi quantitativi di dati.

Se le da ultimo citate tecnologie possono definirsi conquiste quantomeno afferrate, nella misura in cui il Piano Triennale per l'informatica[31] ne fa a ben vedere implicito richiamo, un settore ancora in via d'esplorazione nelle pubbliche amministrazioni è quello degli "smart contracts" (c.d. "contratti intelligenti"). Ebbene, adattare uno schema contrattuale, nato e recepito[32] in ambito civilistico, ad un iniziale rapporto non paritetico – come quello, che qui maggiormente importa, tra stazione appaltante e impresa privata nella fase di formazione del vincolo contrattuale nei procedimenti ad evidenza pubblica – pone anzitutto un problema di innesto dell' "imprinting" informatico[33] tra la determinazione autoritativa (aggiudicazione) e il successivo accordo tra le parti (stipula del contratto), posto che un contratto automatizzato, basato sulla logica sillogistica "if-then", dovrebbe essere pattuito come tale sin dalla sua genesi. Al di là di tali questioni pregiudiziali, che nondimeno necessitano d'essere sciolte per fornire utilità al dibattito, immediati sarebbero i precipitati della scelta di avvalersi di una simile opzione: dal rafforzamento del principio di trasparenza, reso possibile dall'accesso condiviso a tutti i partecipanti alla gara prima, durante e dopo l'esecuzione del contratto, al connesso effetto deterrente di episodi di "maladministration" proprio grazie ad «un'osservazione lineare e continuativa di tutto il processo ancorché libera ed immodificabile che prende a prestito l'innovazione "blockchain" fino ad arrivare all'inibizione e prevenzione di comportamenti irregolari»[34].

Il quadro che si è tentato fin qui di descrivere deve infine essere appuntato con le più recenti novità susseguitesi in materia. Risale allo scorso 18 febbraio 2025 la pubblicazione in consultazione pubblica, da parte dell'Agenzia per l'Italia Digitale (AgID), della bozza di linee guida per l'adozione di IA nella pubblica amministrazione[35]. L'iniziativa si inserisce nell'ambito della Strategia Italiana per l'Intelligenza Artificiale 2024-2026 e mira a fornire un prezioso *vademecum* l'implementazione delle soluzioni digitali nel settore pubblico, in attesa di una normativa nazionale di più ampio respiro. Alla stregua di un documento-filtro, le citate linee guida offrono dettagliate indicazioni per orientare il riferito dinamismo tecnologico delle p.a. all'approccio alla gestione del rischio propugnato dall'AI Act, adombrando le incertezze di disciplina che avrebbero verosimilmente scoraggiato l'innovazione nel timore della non totale conformità ad un contesto normativo in rapida evoluzione.

Oltre l'impostazione multi-valoriale[36], ciò che preme sottolineare in questa sede è, da un lato, il riferimento al riparto di responsabilità e alle misure di sorveglianza umana e, dall'altro, il richiamo al dovere di sviluppo di una strategia per l'IA coerente con il contesto della singola amministrazione. Nella prima prospettiva, una volta segnati i confini tra fornitori ("providers") e utilizzatori ("deployers") e rispettivi obblighi nella catena del valore dell'IA, è di rilievo l'affermazione per cui

[31] https://www.agid.gov.it/sites/agid/files/2025-02/Piano_Triennale_2024-2026_Aggiornamento2025acc_0.pdf.

[32] Invero, sulla spinta della normativa sovranazionale, l'Italia ha riconosciuto lo stato giuridico dello "smart contract" definendolo come «un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse» (art. 8-*ter*.2, D.L. 135/2018 convertito con modifiche nella L. 12/2019).

[33] R. Spina, *L'ipotesi dello* smart contract *nella pubblica amministrazione. Assetti di* governance *dell'innovazione digitale*, in *Rivista Italiana di Public Management* 5.2 (2022) 299.

[34] *Ivi*, 302.

[35] Emanate ai sensi del DPCM 12/01/2024, recante "Piano triennale per l'informatica nella pubblica amministrazione 2024-2026" (https://www.agid.gov.it/sites/agid/files/2025-02/Linee_Guida_adozione_IA_nella_PA.pdf).

[36] Retta dai principi di conformità normativa e governance, di etica e inclusione, di qualità e affidabilità dei sistemi di IA, d'innovazione e sostenibilità, di formazione e organizzazione secondo una pianificazione strategica, *ivi*, 19ss.

«le p.a. adottano l'IA come strumento di supporto all'attività umana consapevoli che la responsabilità ultima delle decisioni adottate, in modo automatico o supervisionato, dai sistemi di IA rimane in capo alla p.a.»[37]. Quanto affermato permette di avvalorare la conclusione a cui si è pervenuti poc'anzi guardando alla sola peculiare conformazione dei piani anticorruzione e non anche alla più recente cornice giuridica: gli stessi piani necessitano di una riferibilità soggettiva che non può essere scaricata sugli algoritmi né il loro pur possibile innesto nella fase di progettazione/monitoraggio va esente da criticità, considerati i rischi riflessi per taluni diritti fondamentali (su tutti la "privacy"), rispetto ai quali l'AI Act prescrive una più intensa protezione.

Dal secondo angolo di visuale, è invece evidente l'accento riposto sulla auto-organizzazione, ancorché indirizzata entro schemi man mano più rigidi e predeterminati in forza del regime del rischio coinvolto (inaccettabile, alto, minimo o limitato)[38], in virtù della quale è la singola p.a. ad individuare i c.d. casi d'uso in cui l'IA offre il massimo beneficio in termini di efficienza operativa ed erogazione dei servizi. Nell'ambito di tale introspezione, assume poi centrale rilevanza la valutazione d'impatto sui diritti fondamentali dei sistemi di IA ad alto rischio (c.d. "fundamental rights impact assessment", FRIA), a testimonianza dell'irreversibile passaggio a logiche regolatrici che partano dal basso (c.d. approccio "bottom-up") benché pur sempre gemmate da una cornice di stretta legalità quale quella del Regolamento europeo[39] in questione.

Con riguardo alle politiche anticorruzione, le amministrazioni potrebbero quindi adottare fin d'ora svariate tecnologie di IA, previo scrutinio (e accurata divulgazione) degli obiettivi e degli ambiti prioritari di applicazione sulla base del proprio contesto. Si pensi, ad esempio, allo sviluppo di modelli predittivi che consentano di adottare decisioni consapevoli e basate su informazioni reali in materie – come l'incompatibilità e il divieto di c.d. "pantouflage" – rispetto alle quali il processamento di dati storici e di addestramento appare quantomai proficuo.

Invero, sebbene a livello di diritto positivo[40] non sia tuttora rinvenibile un esplicito richiamo allo sfruttamento del digitale per finalità preventive – in specie della corruzione –, non può escludersi che, sulla scorta della centralità accordata al "deployer"[41] di sistemi di IA nella fase di implementazione, l'applicabilità dell'AI Act transiti dal versante delle modalità di utilizzo di tali sistemi da parte delle

[37] *Ivi*, 20.

[38] Ci si riferisce agli obblighi che le p.a. – nel ruolo di eventuali fornitori o utilizzatori – devono rispettare in base alla classificazione del rischio dei sistemi di IA adottata dal Regolamento europeo. Cfr. Reg. 1689/2024, artt. 5, 6, 7, 9, 10, 13, 14, 50 (https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:L_202401689).

[39] È infatti noto come l'approccio regolatorio europeo si collochi a metà strada tra i poli opposti dell'autoregolazione statunitense e del dirigismo cinese. Ben lo sottolinea, in generale, M. Colacurci, *Quale diritto penale per l'IA? Alcune riflessioni a partire dalla proposta di regolamento dell'Unione Europea*, in *Jus – Vita e Pensiero* 3 (2023) 359. Più in generale, per un'analisi strutturale del nuovo Regolamento, v. A. Mihai Pop, *Il* risk-based approach*, la* governance *e le sanzioni nell'AI Act*, in *Ciberspazio e diritto* 25.78 (2024) 423ss. nonché, per il relativo *iter legis*, G. Rugani, *La "legge sull'intelligenza artificiale" dell'UE come punto di arrivo e di partenza dei processi di co-regolazione*, in *Osservatorio sulle fonti* 1 (2024) 510ss.

[40] Lo evidenzia Merenda, *L'anticorruzione* cit. 59 il quale rileva come l'AI Act faccia un rapido riferimento alla buona amministrazione, senza affrontare il potenziale impiego di questi strumenti nel campo della corruzione, e che la pendente proposta di direttiva non preveda alcuna norma di collegamento.

[41] Sul punto, il considerando 93 del Regolamento citato, relativamente ai più problematici sistemi ad alto rischio, afferma che: «se da un lato i rischi legati ai sistemi di IA possono risultare dal modo in cui tali sistemi sono progettati, dall'altro essi possono derivare anche dal modo in cui tali sistemi di IA sono utilizzati. I "deployer" di sistemi di IA ad alto rischio svolgono pertanto un ruolo fondamentale nel garantire la tutela dei diritti fondamentali, integrando gli obblighi del fornitore nello sviluppo del sistema di IA. I "deployer" sono nella posizione migliore per comprendere come il sistema di IA ad alto rischio sarà utilizzato concretamente e possono pertanto 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 dei gruppi di persone che potrebbero essere interessati, compresi i gruppi vulnerabili […]».

p.a. e, dunque, nel parallelo incasellamento nelle categorie di rischio sopra richiamate, ad oggi rese più flessibili con la previsione di un sistema di "valvole di sfogo"[42].

3.- **La prevenzione della corruzione quale idealtipo applicativo della c.d. "digital criminal compliance" nel settore privato.**

Di fianco al settore pilota del "trading" finanziario[43], la prevenzione della corruzione si sta sempre più imponendo a terreno elettivo per l'impiego delle nuove tecnologie, anche (e soprattutto) tra gli enti privati. In via generale, è da più parti[44] maturata la consapevolezza, infatti, che se di nuovo volto della "compliance" penalistica vuol parlarsi, non si può di certo trascurare l'impatto della rivoluzione digitale sulla stessa[45]. Per questi motivi, l'attenzione degli studiosi è ora rivolta alla costruzione di un eventuale modello 231 "matematico"[46] in taluni dei diversi ambiti[47] dei reati presupposto.

Come anticipato, quello dell'anticorruzione ben si presta a tale scopo in ragione dell'accentuata densità procedimentalizzata che, se per vero è connaturata agli stessi modelli organizzativi[48], subisce un'amplificazione significativa per via della presenza di una capillare "soft law" di riferimento e di un reticolo di buone pratiche[49]. Queste ultime hanno infatti contribuito, negli ultimi anni, ad indirizzare la "compliance" anticorruzione verso una decisa standardizzazione, incentivata dalle ricadute in punto di premialità *ex post* per l'ente adempiente.

A differenza del settore pubblico, tuttavia, quello privato non si interfaccia con un sistema di banche dati interoperabili bensì con altrettanti ingenti flussi finanziari e di informazione che irradiano la stessa funzionalità del modello 231. Sicché, l'attenta gestione di tale patrimonio informativo, come tale in grado di condizionare il giudizio di idoneità dell'impianto di "compliance", trova nella alternativa digitale un promettente alleato.

Lungi dall'addentrarci in questioni che verranno qui solo intercettate[50], occorre in questa sede riferire delle prassi digitali finora invalse o solo ipotizzate nelle realtà aziendali, distinguendo le innovazioni sulle componenti generali del modello, orientate all'indiscriminata riduzione del rischio-reato, da quelle più propriamente costruite per contenere il rischio corruttivo.

---

[42] Il riferimento è a quanto previsto all'art. 6, par. 3 del citato Regolamento: «In deroga al paragrafo 2, un sistema di IA di cui all'allegato III non è considerato ad alto rischio se non presenta un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche, anche nel senso di non influenzare materialmente il risultato del processo decisionale. […] Fatto salvo il primo comma, un sistema di IA di cui all'allegato III è sempre considerato ad alto rischio qualora esso effettui profilazione di persone fisiche».

[43] Cfr. M. Mozzarelli, *Digital Compliance: The Case for Algorithmic Transparency*, in S. Manacorda, F. Centonze (curr.), *Corporate Compliance on a Global Scale*, Londra 2022, 259ss.

[44] In proposito, si vedano A. Gullo, *Compliance*, in *Archivio Penale* 1 (2023) 12ss; A. Nisco, *Riflessi della* compliance *digitale in ambito 231*, in *Sistema Penale* (2022); G. Morgante, G. Fiorinelli, *Promesse e rischi della* compliance *penale digitalizzata*, in *Archivio Penale* 2 (2022).

[45] In tal senso, V. Mongillo, *Presente e futuro della* compliance *penale*, in *Sistema Penale* (2022) 16.

[46] In questi termini si esprime R. Trezza, *L'intelligenza artificiale come ausilio alla standardizzazione del modello 231: vantaggi "possibili" e rischi "celati"*, in *Giurisprudenza Penale web* 1-*bis* (2021).

[47] Ad es. con riguardo ai reati di criminalità organizzata v. M. Di Florio, *Uno sguardo oltre la* compliance *231:* digital criminal compliance *e rischio di infiltrazioni mafiose nelle imprese*, in *La legislazione penale* (2022); oppure, in tema di reati ambientali v. R. Sabia, *Artificial Intelligence and Environmental Criminal Compliance*, in *Revue Internationale De Droit Pénal* 1 (2020).

[48] In generale sul tema, cfr. A. Gullo, *I modelli organizzativi*, in G. Lattanzi, P. Severino (curr.), *Responsabilità da reato degli enti. Diritto sostanziale*, Torino 2020, 241ss.

[49] Basti qui citare, limitandoci al contesto nazionale, le Linee guida di Confindustria e, per quello internazionale, le certificazioni ISO. Si veda, per tutti, G.M. Evaristi, Soft law *e prevenzione della corruzione d'impresa. Linee guida di Confindustria, Piano Nazionale Anticorruzione e* UNI-ISO 37001, in Gullo, Militello, Rafaraci (curr.), *I nuovi volti del sistema penale* cit. 55ss.

[50] V. *infra* par. 4 e, in particolare, nota n. 85.

Vi è da premettere che, allo stato attuale, l'investimento nel digitale è appannaggio delle grandi imprese[51] per ovvie ragioni legate ai costi e alle risorse umane "da addestrare". Ciononostante, anche in Italia alta è l'attenzione sul potenziale impiego di IA nella costellazione delle piccole e medie imprese, in specie di quella generativa – nelle forme cioè di "software" pronti all'uso, ossia accessibili tramite applicazioni mobili e siti "web", di cui ne costituiscono un esempio ChatGPT (OpenAI), Gemini (Google), Claude (Anthropic), LLaMA (Meta). In suddette realtà, tuttavia, la maggiore attrattività economica delle citate tecnologie si scontra con la bassa maturità digitale e la minore disponibilità di dati[52] che ne rendono al momento più complessa l'adozione.

Analogamente a quanto poc'anzi rilevato dal lato pubblicistico, l'esportata unicità dei modelli 231 – parametrati sui singoli enti – ci sembra frapporsi ad una integrale automazione della "compliance" penalistica. Detto diversamente, difficilmente potrebbe giungersi ad un modello confezionato *in toto* dall'IA, vuoi perché quest'ultima si andrebbe ad innestare in una materia – quella della responsabilità da reato degli enti – storicamente legata alla componente umana ai fini dell'imputazione dell'illecito all'ente[53] vuoi perché, da ultimo, l'AI act ha affermato il criterio del dominio del fattore umano nei sistemi c.d. ad alto rischio.

Alla luce di ciò, sembra convincente l'opinione di quanti preferiscono riferirsi alla "compliance" digitale nell'accezione di "empowerment organizzativo"[54], a voler sottolineare il carattere ancillare della tecnologia rispetto all'insopprimibile supervisione dell'uomo.

Riletto in questa prospettiva – di ormai forzosa incidentalità – l'apporto delle nuove tecnologie sulla progettazione dei modelli è destinato ad un sicuro successo nella fase di mappatura del rischio-reato (anche corruttivo), per le ragioni – già ampliamente ricordate in dottrina[55] – legate alla crescita esponenziale di dati ed informazioni da analizzare, fonti primarie per il "machine learning".

Se, come confermato da prime rilevazioni, il processamento di dati è già realtà in talune delle "major companies", è la correlata tecnologia a registro distribuito – la già menzionata "blockchain" – a chiudere il cerchio che vede nel contenimento del rischio corruttivo una permeabilità all'automazione. La promessa di tracciabilità di ogni transazione, per via della crittografia asimmetrica, gioca infatti un ruolo decisivo nello scoperchiamento di reati (e rispettivi autori) che abbiano ad oggetto somme di denaro. Non pare dunque inverosimile affermare che, alla seria adozione di tali presidi, gran parte dei reati contro la p.a. – e non solo (si pensi, ad esempio, a quei delitti contro l'incolumità pubblica[56] che richiedono la tracciabilità della filiera produttiva) – verrebbero schermati sul nascere.

---

[51] Di sicuro interesse è l'indagine condotta dal Deutsche Institut für Compliance (DICO), a cui hanno partecipato anche Die Allianz für Integrität, UN Global Compact Netzwerk Deutschland (UN GCD) e il Liquid Legal Institute (LLI) sulla diffusione della *digital compliance* a livello globale. Sul punto, v. M. Iannuzziello, Digital Compliance: *un'indagine empirica internazionale su diffusione e prospettive*, in *Corporate Crime & Compliance Hu* (2022).

[52] P. Spagnoletti, T. Volpentesta, *Intelligenza artificiale generativa nelle piccole e medie imprese: evidenze empiriche nel contesto italiano*, in *Rivista di Politica Economica* 2 (2024) 115.

[53] Si veda N. Selvaggi, *Dimensione tecnologica e* compliance *penale: un'introduzione*, in L. Lupária, L. Marafioti, G. Paolozzi (curr.), *Dimensione tecnologica e prova penale*, Torino 2019, 217ss.

[54] Così L. D'Agostino, Criminal compliance *e nuove tecnologie*, in *Diritto penale contemporaneo* 1 (2023) 2.

[55] Per tutti, v. Gullo, *Compliance*, cit. 13 nella parte in cui afferma che «[…] i punti cardinali della "compliance" sono qui rappresentati da dati, flussi finanziari, informazioni». Per una visione più ampia sulla criminalità economica, si rinvia a E. Birritteri, *Corporate criminal liability and new technologies: digital compliance strategies in the fight against economic crimes*, in *The Role of Technology in Preventing and Combating Organized Crime, Financial Crimes and Corruption – Book of Proceedings* (2023) 14ss.

[56] Nello specifico, in tema di sicurezza alimentare (c.p., artt. 440, 442, 517-*quater*) e utilizzo di tecniche "blockchain", v. G. Alesci, *Sicurezza alimentare e nuove tecnologie. I possibili scenari di un rapporto ambiguo*, in Balbi, De Simone, Esposito, Manacorda (curr.), *Diritto penale* cit. 167ss.

Più in generale, è dato registrare nel contesto aziendale[57] un crescente ricorso alla c.d. RegTech, termine "ombrello" – frutto della fusione delle parole "regulation" e "technology" – utilizzato per alludere all'uso della tecnologia con l'obiettivo di rispondere in modo più efficace alle richieste regolatorie e di conformità[58]. Ben si comprende, allora, come nell'era della prevenzione mediante organizzazione – o, se si preferisce, dell'ossessione della previsione, pena il bastone delle sanzioni[59] – prezioso sia il contributo delle soluzioni "smart" nella prognosi dell'esposizione al rischio-reato, la cui accuratezza (o meno) è solita poi transitare nello spartiacque che contrassegna l'"effective" (predisposta ed attuata) dalla "cosmetic" (puramente cartacea) "compliance". Perciò, con specifico riguardo al rischio corruttivo, l'utilizzo dell'apprendimento automatico ("machine learning") per classificare documenti in base ai già citati flussi di denaro, ovvero della biometria comportamentale per registrare le condotte virtuali degli utenti e monitorare i segnali d'allarme di attività fraudolente, o ancora dei modelli semantici in grado di ottimizzare l'estrazione dei dati ("data mining") e generare report in tempo reale permettono, da un lato, di sfruttare virtuosamente il mare magnum dei dati, sempre più ingestibile per le vie tradizionali, e dall'altro di ridurre i costi del personale e dell'intera infrastruttura "software" customizzata ("software custom"). Non da ultimo, tali strumenti potrebbero intervenire anche a valle della fase di progettazione del modello organizzativo, garantendone il controllo e l'aggiornamento senza soluzione di continuità.

Spostandoci verso una delle misure originariamente adottate nel settore dell'anticorruzione e successivamente transitata a presidio del più generale malaffare[60] – il "whistleblowing" – variegati sarebbero gli impieghi dell'IA: dal riepilogo automatico delle segnalazioni alla trascrizione dei "file" audio nei casi di utilizzo di servizi di "voice messaging"; dall'eventuale traduzione automatica alla sua anonimizzazione. In questo senso, va da sé che ad una proficua attivazione dei canali di segnalazione, comprensiva delle tutele legali previste per il "whistleblower", corrisponda tanto il "successo" pratico dell'istituto – sospeso nel difficile bilanciamento tra l'incentivo all'emersione "dal basso" di condotte illecite e il disincentivo alla denuncia facile, di qualsiasi presunta irregolarità – quanto l'aderenza del modello al dato normativo che, nel prescriverne l'adozione (v. art. 6, c. 2-*bis*, D.Lgs. 231/2001), è giocoforza calibrata sulle possibilità di esenzione da responsabilità penale ovvero di premialità *post delictum* dell'ente comunque "compliant".

Tanto premesso, conviene ora concentrare l'attenzione sulle cautele specifiche di settore.

Si è già ampiamente segnalata la centralità dei flussi informativi per la "compliance" digitale. Nel campo dell'anticorruzione, tuttavia, questi ultimi assumono una valenza ancora più pregnante poiché idonei ad influenzare a cascata la qualità delle prestazioni della funzione anticorruzione (ove presente) e di quella di "audit", nonché dell'eventuale società di revisione e dell'Organismo di vigilanza (OdV). In un esempio: è noto come il reato di falso in bilancio, storica fattispecie grimaldello nella lotta alla corruzione, tragga alimento dalla costituzione di una provvista illecita, che proprio nella opacità dei flussi informativi tra i plessi societari può essere illecitamente celata e dar luogo a forme concorsuali

[57] Per tutti, si vedano le soluzioni adottate da PwC: https://www.pwc.com/it/it/publications/assets/docs/pwc-regtech.pdf.

[58] È questa la definizione di RegTech fornita dell'Institute of International Finance, v. IIF, *Regtech in Financial Services: Technology Solutions for Compliance and Reporting* (2016) 2.

[59] Ci si riferisce al noto "stick and carrot approach" per cui, nell'ambito del D.Lgs. 231/2001, al bastone dalla pena per l'insufficiente predisposizione di una "compliance" preventiva finalizzata a minimizzare il rischio-reato si affianca la carota della impunità per le imprese dotate di un adeguato modello organizzativo in grado di impedire – nel contesto che qui interessa – l'attività corruttiva dei loro operatori.

[60] La relativa disciplina, come noto, ha avuto un primo riconoscimento in ambito pubblicistico (con la L. 190/2012 che ha inserito l'art. 54-*bis* all'interno del D.Lgs. 165/2001), salvo poi espandersi anche nel settore privato (L.179/2017) e trovare infine armonizzazione nel D.Lgs. 24/2023.

di responsabilità penale. Ragion per cui la già ricordata tecnologia "blockchain", oltre che il *quid alii* "cloud computing" – benché tacciato di estrema dipendenza dai (deboli) sistemi "provider"[61] – potrebbero contribuire al raggiungimento di un'adeguatezza "by default" dei flussi informativi.
Seguendo questa traccia argomentativa, è stato altresì evidenziato[62] come la costruzione di una "blockchain" privata e "permissioned" – che sfrutti cioè la strutturazione in blocchi del registro distribuito tra soli "nodi" interni all'ente (singole funzioni, organi gestori e di controllo) – possa esplicare i suoi effetti in due opposte direzioni: anticipatoria, a rafforzamento della "compliance" predittiva, e postuma, a supporto di eventuali investigazioni interne e di forme di collaborazione con l'Autorità giudiziaria.
Rispetto alla gestione delle disposizioni di pagamento in uscita dall'ente, invero, l'utilizzo di simili presidi digitali – dotati delle caratteristiche della immodificabilità – potrebbe ridurre il rischio di comportamenti appropriativi, distrattivi e corruttivi che verrebbero inabilitati dallo sbarramento tecnico[63] a determinate operazioni, non conformi ai protocolli aziendali e come tali in grado di destare segnali d'allarme precocemente neutralizzabili.
Nel complesso, la procedimentalizzazione delle attività aziendali in nome di standard normativi (es. soglie, divieti) avrebbe il pregio di limitare alla fonte la possibilità d'agire[64] dei soggetti apicali o sottoposti. In tale direzione, la gestione di fondi PNRR, ovvero di altre risorse di derivazione statale o europea, potrebbe divenire il diretto destinatario di questa barriera all'entrata, con vantaggi evidenti per la "messa a terra" degli investimenti e delle politiche di transizione programmate.
Ulteriori applicazioni dell'IA nel contesto della "compliance" anticorruzione potrebbero, infine, riguardare una varietà di altri presidi, che ben si presterebbero a forme di automazione.
Sul terreno delle sponsorizzazioni, dell'omaggistica e delle donazioni, si pensi ai benefici delle numerose tecnologie di IA ("blockchain", "machine learning", "advanced analytics") nella determinazione della rotazione temporale e della parte premiale della retribuzione da destinare a tali scopi nonché nella predeterminazione e immodificabilità in itinere del "budget" annuale a ciò deputato.
Avuto riguardo al sistema di qualifica dei fornitori, invece, innegabili sarebbero i vantaggi della implementazione di una rete "blockchain" – questa volta ibrida, fatta di "nodi" interni ed esterni all'ente, di cui questi ultimi agganciati a reti pubbliche – nel condurre verifiche, e annesse analisi reputazionali, sulle potenziali infiltrazioni criminali nelle aziende partner, che spesso sottendono un più generale "screening" sui fenomeni corruttivi. In tal senso, già lo standard internazionale ISO 37001 – imponendo la pianificazione di processi di "due diligence" sui soci in affari per valutare il rischio corruzione – sembra aprire all'utilità dei programmi di "decision intelligence" per le analisi su tali fonti aperte[65].
Ancora, proprio l'affinamento della procedura di "due diligence" nei confronti delle terze parti, resa possibile dall'apporto del digitale, gioverebbe in particolar modo alla prematura emersione di taluni reati avamposto e reati spia in senso lato, quale il (da ultimo novellato) traffico di influenze illecite[66]

[61] Si veda, in proposito, il rapporto dal titolo *Top Threats to Cloud Computing 2024* della Cloud Security Alliance (CSA): https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2024.
[62] A. Gullo, R. Sabia, *Intelligenza artificiale e* compliance *penale. Scenari attuali e prospettive evolutive*, in *Rivista di Politica Economica* 2 (2024) 157.
[63] Morgante, Fiorinelli, *Promesse* cit. 11.
[64] Gullo, Sabia, *Intelligenza* cit. 155.
[65] D'Agostino, *Criminal compliance* cit. 7.
[66] In proposito, v. A. Gullo, *I reati contro la pubblica amministrazione e a tutela dell'attività giudiziaria*, in Lattanzi, Severino (curr.), *Responsabilità* cit. 445 nella parte in cui afferma che «[…] qui il rischio, alla luce dell'inclusione tra i

e l'autoriciclaggio[67], entrambi ricompresi nel novero dei reati presupposto del decreto 231. In tale contesto, lo schema sillogistico degli "smart contracts" potrebbe essere replicato per concludere, preventivamente, dei c.d. patti etici tra le imprese "partner". Questi ultimi, per mezzo della automazione delle clausole sul rispetto dei requisiti d'integrità e trasparenza e di esclusione/decadenza dai rapporti commerciali al ricorrere di circostanze predeterminate, tracciabili anche dall'incrocio con le banche dati pubbliche, potrebbero altresì rappresentare un freno significativo alla polimorfia offensiva[68] del reato di corruzione tra privati, parimenti incluso nel catalogo dei reati presupposto della responsabilità *de societate*.

Non da ultimo, in parallelo a quanto ipotizzabile nel settore pubblico, anche in quello privato la tecnologia "blockchain" ibrida potrebbe soccorrere nel tracciamento di conflitti di interessi e periodi di raffreddamento (c.d. "black period") per ex pubblici agenti che aspirino a posizioni manageriali negli enti privati in favore dei quali hanno emanato provvedimenti.

Le procedure di selezione del personale – che vengono qui in rilievo, sia pure dal lato della prevenzione dei fenomeni corruttivi – permettono infine di svolgere talune considerazioni conclusive *de iure condito* e *condendo*. Se, ad oggi, è consentito partire da una inequivoca premessa di fondo, in base alla quale "un sistema di IA di cui all'allegato III [ndr. del Regolamento (UE) 2024/1689] è sempre considerato ad alto rischio qualora esso effettui profilazione di persone fisiche" (art. 6, par. 3, Regolamento cit.) e che parimenti ad alto rischio sono i sistemi di IA «destinati a essere utilizzati per l'assunzione o la selezione di persone fisiche, in particolare per pubblicizzare i posti vacanti, vagliare o filtrare le candidature, valutare i candidati nel corso di colloqui o prove» (allegato III, n. 4, lett. a) del Regolamento cit.), con la ripartizione di obblighi che ne consegue, in specie sull'ente-"deployer" (v. art. 26 Regolamento cit.), altrettanto non può apriori affermarsi per le altre misure anticorruzione potenzialmente interessate all'innesto di IA.

In altre parole, con riferimento a queste ultime, andrebbe allo stato vagliato caso per caso se, e in che misura, l'utilizzo di sistemi di IA sia comunque classificabile ad alto rischio, secondo i dettami dei ricordati art. 6 e allegato III del Regolamento, con applicazione dei più stringenti obblighi in capo agli attori coinvolti nella catena del valore dell'IA.

In definitiva, nell'attesa del completamento della normativa, europea – si veda, in particolare, quanto statuito all'art. 6, par. 5, Regolamento («dopo aver consultato il consiglio europeo per l'intelligenza artificiale […], ed entro il 2 febbraio 2026, la Commissione fornisce orientamenti che specificano l'attuazione pratica del presente articolo […] insieme a un elenco esaustivo di esempi pratici di casi d'uso di sistemi di IA ad alto rischio e non ad alto rischio») e nazionale, un "leitmotiv" dal quale si può difficilmente prescindere, per cercare di adempiere a tale arduo compito, è il richiamo ai rischi di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche.

reati presupposto del traffico di influenze illecite, è quello di consulenti che ricerchino contatti illeciti con pubblici agenti (o, come emerso nelle dinamiche della corruzione internazionale, siano beneficiari di incarichi che in realtà celino dazioni indebite), o di società partner che siano oggetto di valutazione ai fini dell'acquisizione o di fusioni in considerazione del rischio per l'ente di doversi fare carico di future sanzioni), o di controllate, anzitutto estere, rispetto alla possibilità della risalita della responsabilità in ipotesi di corruzione posta in essere da un suo apicale o sottoposto».

[67] Per un'analisi sull'uso degli algoritmi nella "compliance" antiriciclaggio, v. A. Esposito, *Note sparse sull'intelligenza artificiale*, in Balbi, De Simone, Esposito, Manacorda (curr.), *Diritto penale* cit. 46ss. nonché, più in generale, V. Plantamura, *Il cybericiclaggio*, in Cadoppi, Canestrari, Manna, Papa (curr.), *Cybercrime* cit. 941ss.

[68] Così A. Tripodi, *La corruzione tra privati. Un'analisi diacronica dello spettro offensivo della fattispecie ovvero la concorrenza come figlia di un dio minore*, in *Discrimen* (2018) 3 per alludere allo spettro offensivo del reato, che può spaziare dalla lealtà concorrenziale all'integrità economico-patrimoniale della società.

4.- **(In)esistenza di un punto di equilibrio: prospettive attuali e future dell'anticorruzione automatizzata tra sfera pubblica e privata.**

Volendo tirare le fila del discorso – tutt'altro che privo di implicazioni pratiche – non può non convenirsi con l'idea che a fare da bussola, in tale processo di gestazione verso una normativa che detti le "regole del gioco"[69], sia la ratio ispiratrice dell'urgenza regolatoria europea, rinvenibile nella creazione di un costituzionalismo digitale comune[70] e del suo nocciolo duro.

Partendo da questa base, finalizzata a salvaguardare i diritti fondamentali dai rischi connaturati nell'utilizzo di IA, gli utilizzatori di tali tecnologie – siano essi p.a. o enti privati – saranno comunque tenuti ad inventariare i sistemi impiegati (o che si programma di impiegare) e inquadrarli alla luce della classificazione del rischio già richiamata[71], e ciò a prescindere da una precisa disposizione che ne prescriva di volta in volta il c.d. "impact assessment". Invero, acclarata l'essenzialità dei "deployer" nell'individuazione di potenziali rischi significativi non previsti nella fase di sviluppo del sistema[72], i campi applicativi dell'IA sin qui elencati appaino, nella quasi totalità, in vario modo in frizione con la tutela di alcuni diritti primari. Da ciò ne consegue l'inclusione nei sistemi ad alto rischio[73], rispetto ai quali l'innalzamento dello scudo costituzionale è, come detto, più forte.

Se l'obiettivo ultimo (almeno dichiarato) è stato quello di pervenire ad un testo legislativo "future proof", in grado di adattarsi all'evoluzione tecnologica[74], con rinuncia a disciplinare uno o più specifici settori al fine di rivolgersi all'IA trasversalmente[75], i punti cardinali attraverso i quali orientarsi sono rappresentati proprio dai diritti fondamentali e dalla loro tutela, onde garantire traduzione pratica all'approccio antropocentrico che ha animato il fervore normativo del legislatore europeo.

Ebbene, tanto l'automazione di taluni aspetti dei piani anticorruzione quanto l'implementazione di una "compliance" digitale, sub-specie anticorruzione, negli enti privati si prestano a forme occulte di controllo a distanza delle risorse umane[76], per non dire delle violazioni al diritto alla riservatezza dei

[69] Espressione utilizzata da V. Mongillo, *Responsabilità da reato degli enti e crimini connessi all'intelligenza artificiale: tecniche giuridiche di intervento e principali ostacoli*, in *Archivio penale* 2 (2024) 18.

[70] Sul tema, si rinvia a O. Pollicino, *Di cosa parliamo quando parliamo di costituzionalismo digitale?*, in *Quaderni costituzionali* 3 (2023) 569ss.

[71] In questi termini, Gullo, Sabia, *Intelligenza artificiale* cit.164 i quali fanno l'esempio 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"».

[72] Si riportano nuovamente le parole Reg. (UE) 2024/1689, considerando 93.

[73] Già Nisco, *Riflessi della* compliance *digitale in ambito 231* cit. 8 prevedeva un simile inquadramento al momento della proposta di Regolamento in esame.

[74] Si veda però la criticità evidenziata da F. Consulich, *Il diritto penale al tempo dell'intelligenza artificiale. Prospettive punitive nazionali dopo l'AI Act*, in *Diritto di Difesa – Rivista dell'Unione delle Camere penali italiane* (2024) 13 il quale afferma che: «la categorizzazione impiegata, che sostanzialmente identifica una scala decrescente di rischio, ha una conformazione statica, realizza cioè una fotografia di alcuni tipi di intelligenze artificiali che di per sé possiedono un coefficiente di dannosità potenziale. Non si coglie però la possibilità che sia le attività menzionate negli allegati al Regolamento sia quelle che nemmeno vi compaiono, perché ritenute non pericolose o perché non ancora entrate sulla scena, "saltino di scala": apprendano, in via esperienziale, una potenzialità lesiva che in origine non avevano (o meglio: non sapevano di avere). Dunque, la classificazione operata a priori dal regolatore europeo potrebbe presentare profili di rapida obsolescenza e trovarsi così ben presto anacronistica: sono definiti solo in sede tecnica i meccanismi di adeguamento della disciplina, in assenza di criteri individuati dal legislatore con scelte politiche».

[75] Mihai Pop, *Il* risk-based approach cit. 425.

[76] Diffusamente sul tema, v. A. Nisco, *Prospettive penalistiche del controllo a distanza sull'attività lavorativa nell'attuale contesto normativo e tecnologico*, in *Diritto penale contemporaneo* 4 (2021) 89ss; E. Birritteri, *Controllo a distanza del lavoratore e rischio penale*, in *Sistema Penale* (2021).

dati personali e della potenziale compromissione dei c.d. neurodiritti[77], alla stregua di facce di uno medesimo fenomeno che è stato ribattezzato sotto il nome di "capitalismo della sorveglianza"[78].
In effetti, strumenti quali il "machine learning" (anche nella sua versione "deep") in combinazione con l' "advanced analytics" per scrutinare interi comparti documentali, la biometria comportamentale, la "decision intelligence" su fonti aperte fino ad arrivare alla tutt'altro che utopica "predictive policing" privata[79] addestrata per fornire indicazioni su eventuali futuri comportamenti illeciti dei dipendenti da un lato, e i processi decisionali digitalizzati dall'altro – come quelli in sperimentazione nell'ambito degli appalti pubblici – presentano rischi significativi per gli individui e gli operatori economici.
Per i primi – con tutta evidenza il personale aziendale coinvolto nei processi a rischio reato – incombe il pericolo di un tracciamento indiscriminato del traffico "e-mail", delle chiamate telefoniche o telematiche, dei "file" di navigazione, delle coordinate GPS, ecc. Rischi che, in realtà, innervano la più generale transizione al digitale della "compliance" penalistica, in specie qualora le nuove tecnologie siano utilizzate per la prevenzione dei reati. Una esasperazione della componente predittiva, invero, nel segno dell'incentivo alla serrata emersione di fatti illeciti, aprirebbe le porte a fenomeni distorsivi, in grado di azzerare quanto di buono è insito nell'automazione. Si pensi all'incognita rappresentata dai "bias" cognitivi e, dunque, ai connessi episodi di discriminazione algoritmica a cui verrebbe esposto il personale preposto alle mansioni a più altro rischio corruttivo; oppure alla moltiplicazione dei rischi che, dall'essere inizialmente confinati entro un piano di governo, si ritrovano indisciplinati e sguarniti di presidi a seguito dell'attivazione di altre violazioni (come quelle al GDPR in caso di dati personali), per così dire di secondo livello[80], perpetrate proprio per mezzo dalla componente digitale.
Per i secondi, invece, si nasconde il rischio di una schedatura perenne, per quanto incompleta e ancorata al passato e, perciò, potenzialmente lesiva dei principi che governano le procedure di gara. La spinta verso l'interoperabilità delle banche dati pubbliche, in effetti, se da un lato avrebbe il merito di attualizzare il criterio del c.d. "once only" – per il quale, in un'ottica di semplificazione, l'operatore economico è tenuto ad inserire solo una volta i documenti richiesti sul proprio fascicolo virtuale, spostandosi poi sull'amministrazione l'onere di recuperare le informazioni nelle successive procedure – dall'altro esporrebbe le imprese, nelle fasi di controllo, a monitoraggi basati sul riutilizzo dei dati, con connessi problemi di riservatezza e inattualità delle informazioni rese alla p.a. durante una delle possibili procedure ad evidenza pubblica alle quali le stesse potrebbero partecipare[81].

[77] Per tali si intendono i diritti umani relativa alla sfera cognitiva. Sul tema, si veda A. Nisco, *Le neurotecnologie assistite dall'intelligenza artificiale nell'ottica del diritto penale*, in *La legislazione penale* (2024) 5ss.
[78] Si veda Selvaggi, *Dimensione tecnologica e* compliance *penale* cit., nella parte in cui afferma che «il capitalismo è entrato in una nuova fase: quello della sorveglianza» e Morgante, Fiorinelli, *Promesse e rischi della* compliance *penale digitalizzata* cit. 27 le quali a loro volta citano il lavoro pionieristico di S. Zuboff, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Roma 2019.
[79] In proposito, v. Morgante, Fiorinelli, *ibidem* e Nisco, *Riflessi* cit. 7.
[80] In questi termini Birritteri, *Corporate criminal liability and new technologies: digital compliance strategies in the fight against economic crimes* cit. 17-18 laddove afferma che «[…] These are, in short, activities that, while aimed at avoiding risks for companies, may generate additional and different legal risks – we might say, of a secondary or indirect nature – from those that they aim to contain and manage».
[81] In tema, E. Carloni, *Qualità dei dati,* big data *e amministrazione pubblica*, in R. Cavallo Perin (cur.), *L'amministrazione pubblica con i* big data*: da Torino un dibattito sull'intelligenza artificiale*, Torino 2021, 475, nella parte in cui afferma che «[…] è necessario tenere sempre presente che alcuni dati possono essere "veri" e completi per alcune procedure e i loro usi primari, ma imprecisi per altre».

Ma ulteriori sono le criticità: dalla qualità, veridicità ed esaustività del "data set" – precondizione per l'eventuale impiego di IA nel contrasto alla "maladministration" nelle procedure di gara, onde evitare un addestramento scorretto degli algoritmi e la restituzione di un "output" ingiustificatamente discriminatorio – al problema noto come "model myopia", insito nell'utilizzo di tecniche di data mining, laddove si cela il pericolo di un'ostinata messa a fuoco, da parte dei controllori, sui comportamenti pregressi dell'operatore economico, magari sovraccaricandolo di verifiche, perdendo però il *focus* generale su possibili nuovi rischi di "maladministration"[82].

Come noto, tuttavia, quello dei dati è un nodo centrale su cui convergono i più disparati tentativi d'innesto dell'IA, dalla diagnosi medica alla sperimentazione di auto a guida autonoma. Anche in questa sede, il problema riaffiora da più punti di vista come quello, finora non menzionato, delle indagini interne alle organizzazioni complesse, supportate dalla tecnologia, rispetto alle quali la più attenta dottrina[83] ha sottolineato la tensione con il diritto di difesa dell'ente stesso, che potrebbe poi trovarsi al cospetto di una prova digitale precostituita ancorché all'evidenza parziale e/o viziata da "bias" cognitivi.

Riconosciuti i rischi ("perils") e note le promesse ("promises")[84] di un'anticorruzione automatizzata – queste ultime abbreviabili nella maggiore effettività dei paradigmi di contrasto – occorre guardare, infine, ai modi di governo dei primi in funzione della valorizzazione delle seconde. Non va neppure dimenticato, in proposito, che per gli enti privati il ricorso ad una "compliance" digitale, con le cadenze sopra elencate, si presenta come un'occasione per veicolare in positivo il giudizio di conformità del modello 231 in sede giudiziaria, tema su cui la dottrina[85] si sta interrogando a più riprese.

Come detto, la risposta che ora può fornirsi risiede nell'attivazione delle più stringenti cautele previste dall'AI Act per i sistemi ad alto rischio. Le amministrazioni e gli enti privati, pertanto, nella qualità di eventuali utilizzatori delle tecniche di IA analizzate, e previo "impact assessment" sui rischi per gli utenti, dovranno uniformarsi agli obblighi previsti all'art. 26 del Regolamento cit. riconducibili a quattro macrocategorie[86].

Per finire, e senza pretesa d'esaustività, si vogliono spendere delle parole conclusive sul cuore del problema algoritmico: l'autonomia decisionale che taluni sistemi di IA possono acquisire in corso di addestramento. Si allude, cioè, alla bipartizione tra algoritmi deterministici e non deterministici, là

[82] Ballerini, *La digitalizzazione* cit. 7.

[83] Nisco, *Riflessi* cit. 8.

[84] Si vuol qui riprendere la struttura del lavoro di N. Köbis, C. Starke, I. Rahwan, *The promise and perils of using artifical intelligence to fight corruption*, in *Nature Machine Intelligence* (2022).

[85] Il riferimento è alla proposta di C. Piergallini, *Premialità e non punibilità nel sistema della responsabilità degli enti*, in *Diritto penale e processo* 4 (2019) 536 il quale ritiene che i modelli 231 conformi allo standard del settore (in questo caso "best practices*"* anticorruzione integrate a tecniche di IA) dovrebbero essere assistiti da una presunzione *iuris tantum*, di idoneità preventiva, superabile dal giudice solo attraverso l'assolvimento di un onere motivazionale rafforzato; tesi poi ripresa, tra gli altri, da Gullo, *Compliance* cit. 16; D'Agostino, *Criminal compliance* cit. 5 nonché da ultimo, da L. Fimiani, *La tecnologia nel sistema penale: dalla giustizia predittiva alle problematiche sull'utilizzo della "IA" per prevenire episodi criminosi*, in *Discrimen* (2024) 10ss.

[86] Sinteticamente: i) gestione del rischio mediante l'adozione di idonee misure tecniche e organizzative a garanzia dell'utilizzo dei sistemi; ii) sorveglianza umana; iii) monitoraggio e "reporting", a cura del "deployer", delle circostanze in cui si ravvisi un rischio per la salute, la sicurezza o i diritti fondamentali delle persone, ovvero si verifichi un incidente grave; iv) trasparenza, informazione e documentazione, declinata nel contesto di lavoro in una informativa *ex ante* ai lavoratori interessati e ai loro rappresentanti, da parte del "deployer"- datore di lavoro, e per i sistemi di IA ad alto rischio che adottano (o assistono nell'adozione di) decisioni che riguardano persone fisiche, una informativa a queste ultime. Oltre al dato normativo, v. Gullo, Sabia, *Intelligenza artificiale* cit.165 e cfr. Bozza di linee guida per l'adozione di IA nella pubblica amministrazione cit. 28ss.

dove i primi, al contrario dei secondi, applicano un metodo statistico-probabilistico per effettuare una previsione, il cui esito è sia incerto *ex ante* che difficilmente intelleggibile *ex post* (c.d. effetto "black box").

Nella consapevolezza che gran parte dei sistemi di IA sono utilizzati (e ovviamente prodotti) da persone giuridiche, bisogna nondimeno tenere distinti i piani delle pubbliche amministrazioni e degli enti privati, limitandoci al caso in cui questi ultimi assumano il ruolo di "deployer".

Sebbene il dibattito sia tutt'altro che saturo[87], per le prime si auspica di risolvere il problema in radice, sul fronte della qualità dei dati, declinati nella duplice funzione di corollario del principio di non discriminazione algoritmica[88] e di ulteriore interesse pubblico che la p.a. deve curare e perseguire. Di qui, la teorizzazione della c.d. riserva di umanità[89] che vorrebbe il recupero del ruolo di decisore del funzionario, con sua conseguente responsabilizzazione, e dell'apporto partecipativo dei privati. Si tratta, del resto, di quanto affermato nella richiamata Bozza di linee guida per l'adozione di IA nelle pubbliche amministrazioni e alla quale si rimanda.

Sul fronte penalistico, la questione si fa più complessa in quanto ci si appresta a discutere di un tema che passa sul crinale della responsabilizzazione degli enti-"deployer" per "algorithmic misconduct". In altre parole, *quid iuris* per l'ente che si avvalga di sistemi di IA completamente autonomi e non programmati/utilizzati per commettere reati ma che, ciononostante, vengano da questi commessi in virtù di una decisione autonomamente assunta, rispetto alla quale né il progettista né il programmatore né l'utente finale possono conoscere esattamente e in anticipo il "pattern" comportale che la macchina ha seguito[90]?

È questo, a ben vedere, un tema che solo in parte intercetta le nuove manifestazioni corruttive – perpetrabili per mezzo degli algoritmi – ma che finisce per assestarsi su un più generale piano di governabilità dell'IA per mezzo del diritto, anche penale. Relegato alla sua funzione di *extrema ratio*, quest'ultimo potrebbe subentrare a valle di una regolamentazione puntuale in materia di circolazione dei prodotti digitali con sanzioni effettive, dissuasive ed efficaci volte a colpire la *societas* per omessa prevenzione dei danni verificatisi a causa dell'utilizzo del dispositivo di IA, benché *ex ante* calcolabili per via delle correnti conoscenze tecnico-scientifiche.

In definitiva, l'avvento degli strumenti digitali quali nuovi e promettenti "anti-corruption tools" procede di pari passo con l'avanzare della dominabilità giuridica dell'IA, nell'ambizioso per quanto urgente tentativo di supervisionare la tecnologia con la tecnologia stessa.

[87] Per quanto qui d'interesse, si esula dalle questioni legate all'utilizzo degli algoritmi nell'attività provvedimentale della pubblica amministrazione, per questi aspetti v. G. Clemente di San Luca, M. Paladino, *Decisione amministrativa e intelligenza artificiale*, in *Federalismi.it* 4 (2025).

[88] Si riveda Cons. Stato, Sez. VI, 13/12/2019, n. 8472 laddove si afferma la necessità di «rettificare i dati in 'ingresso' per evitare effetti discriminatori nell'*output* decisionale».

[89] Si veda l'autorevole saggio di J. Ponce Solè, *Inteligencia artificial, Derecho administrativo y reserva de humanidad: algoritmos y procedimiento administrativo debido tecnológico*, in *Revista General de Derecho Administrativo* 50 (2019).

[90] Per un'accurata ricostruzione sul tema, si rimanda a Mongillo, *Responsabilità da reato degli enti e crimini connessi all'intelligenza artificiale* cit. 5ss. il quale opportunamente tiene distinti i casi di sistemi di IA non autonomi – rispetto ai quali possono essere attivati gli "ordinari" canali di "enforcement" e di imputazione delle responsabilità penali all'individuo ed eventualmente anche alla persona giuridica – e le ipotesi di sistemi autonomi deliberatamente utilizzati per commettere reati – rispetto ai quali gli applicativi di IA si pongono come una sorta di *longa manus* degli autori che li intendano perpetrare e che pertanto saranno loro individualmente attribuibili ovvero, ove ciò sia possibile, imputabili alla persona giuridica entro la quale sono incardinati, qualora quest'ultima risulti interessata o avvantaggiata dalla commissione dei medesimi reati.

Abstract.- Quale terreno a più alta sperimentazione procedimentalizzata, la prevenzione della corruzione nelle organizzazioni complesse – siano esse pubbliche amministrazioni o enti privati – ben si presta all'innesto di nuove tecnologie in grado di ottimizzare i nativi processi analogici (c.d. "paper-based"). In vista di una mirata applicazione dell'AI act, il contributo intende, da un lato, mettere in luce i vantaggi dell'utilizzo di tali tecnologie nella costruzione dei modelli anticorruzione e, dall'altro, segnalare i rischi connessi ad una loro impregiudicata implementazione, non curante della tutela di altri interessi difficilmente (o praticamente non) negoziabili.

As an area of greater procedural experimentation, corruption prevention in complex organizations – whether public administrations or private entities – is well suited to the implementation of new technologies capable of optimizing the native analog processes (paper-based). In view of a targeted application of the AI Act, the paper aims, on the one hand, to highlight the advantages of using these technologies in the anti-corruption models and, on the other, to stress the risks associated with their unprejudiced implementation, disregarding the protection of other interests that are difficultly (or practically non-) negotiable.