NOTA INFORMATIVA N. 15/2021

COMPLIANCE ANTICORRUZIONE IMPRESA

1. *Compliance* e nuove tecnologie di contrasto alla corruzione

Attualmente sia le imprese private (specie se di notevoli dimensioni), sia le pubbliche amministrazioni devono fare i conti con una grande mole di dati eterogenei e prodotti in tempo reale. Tale tipologia di dati (i c.d. big data) proprio per queste caratteristiche non possono essere gestiti attraverso le tradizionali metodologie di archiviazione e analisi, ma necessitano inevitabilmente dell'ausilio delle nuove tecnologie (v. sul punto il Libro Bianco dell'Agenzia per l'Italia Digitale del marzo 2018, L'intelligenza artificiale al servizio del cittadino, p. 52). Ben si comprende, quindi, come ciò rappresenti un rilevante problema di governance per i soggetti coinvolti.

Nondimeno, i recenti sviluppi della prassi in materia dimostrano che esiste la possibilità di trasformare dati asettici in informazioni rilevanti per la prevenzione del rischio corruzione. Insomma, quello che emerge in via embrionale è che la gestione dei dati più che rappresentare un problema può in realtà divenire un'interessante opportunità per i settori privato e pubblico, due mondi apparentemente lontani ma che negli ultimi tempi fanno registrare una sempre maggiore osmosi di idee e *best practice* nelle attività di *enforcement* anticorruzione. Osmosi resa possibile anche dall'atteggiamento proattivo di molte realtà imprenditoriali private che, in alcuni casi, hanno sviluppato innovativi meccanismi di prevenzione dei fenomeni corruttivi. E ciò anticipando le stesse scelte di regolazione del legislatore, superando l'esistenza di obblighi cogenti. Proprio tale fenomeno si è manifestato con palmare evidenza nell'uso di sistemi di *big data analytics* nell'ambito delle attività di monitoraggio e gestione del rischio corruzione.

Da qualche anno, infatti, specie nel sistema anglosassone si sono implementati strumenti informatici automatizzati di raccolta, confronto e analisi – anche mediante l'uso di algoritmi e *software* di intelligenza artificiale – di una rilevante quantità di dati interni ed esterni all'impresa, in particolare in una triplice direzione:

- identificare rilevatori di anomalia, rischio corruzione e ulteriori segnali d'allarme nelle operazioni aziendali (in particolare: azioni anomale rispetto ai modelli di comportamento che il sistema qualifica come ricorrenti/ordinari)
- monitorare il traffico *mail* interno, allo scopo di individuare conversazioni in cui si utilizzino determinate parole chiave considerate "a rischio"
- fornire al *management* un *report* in *real-time* in merito a eventuali profili di anomalia (o altri *red flags*) nel comportamento del (o nei dati raccolti sul) *partner*/agente con cui sono in corso determinate operazioni (c.d. *third party due diligence*).

I *red flag* oggetto di attenzione sono numerosi. Essi vanno, solo per citarne alcuni, dall'identificazione di prezzi d'acquisto, compensi per consulenze e flussi di denaro anomali rispetto alla media dei prezzi di riferimento del settore commerciale e dell'area geografica, all'individuazione di segnali (d'allarme) di possibili conflitti di interesse tra esponenti delle funzioni aziendali coinvolte nelle transazioni e terze parti, fino a movimenti finanziari sospetti rispetto alla "storia" di *business* dell'impresa.

Si tratta, del resto, di procedure e prassi operative che rappresentano soltanto una parte di un ideale mosaico complessivo la cui immagine ci restituisce chiara l'idea di come ormai il tema dell'intelligenza artificiale abbia fatto ingresso in vari settori del sistema penale: dalla prevenzione pubblica dei reati (c.d. *predictive policing*) attraverso *software* intelligenti in grado di individuare aree territoriali in cui vi è maggiore probabilità di attività delittuose o di aiutare gli inquirenti a selezionare, tra milioni di file, quelli più "pro- mettenti" per l'indagine; fino all'esercizio della giurisdizione, con l'utilizzo di algoritmi in grado di identificare il rischio di recidiva di determinati soggetti, supportando il giudice nella propria attività di *Sentencing*.

Le straordinarie potenzialità di questi strumenti hanno fatto sì che fossero utilizzati nelle attività di prevenzione del rischio reato (e in particolare del rischio corruzione) nell'ambito di strutture complesse. Ben poco però si è, sino a ora, riflettuto sulla possibilità che lo sviluppo di tali procedure possa portare a una vera e propria metamorfosi del volto attuale della compliance privata e pubblica: da un sistema che ruota attorno alle classiche attività umane di analisi e indagini preventive "sul campo", a un sistema automatizzato in cui è la sola "macchina" ad assumere su di sé il ruolo di valutare il rischio e di individuare le procedure per gestirlo – e in cui l'uomo svolge soltanto il compito di assicurarsi che il software intelligente abbia riserve di "carburante" (cioè dati) sufficienti a poter svolgere i propri adempimenti di sorveglianza.

Si pensi, per esempio, anche alle prospettive che si stanno aprendo in termini di utilizzo della tecnologia *blockchain* per aumentare la trasparenza e la verificabilità dei dati e dei processi interni alle organizzazioni – con risvolti potenzialmente rivoluzionari anche per il contrasto alla corruzione, ancora del tutto inesplorati.

2. *Compliance* anticorruzione impresaria e *Big Data Analytics*

Volgendo lo sguardo al settore della compliance anticorruzione privata si ritiene che siano identificabili alcuni temi principali.

(A) Innanzi tutto, dalla prassi sembra emergere come siano le singole società a decidere come strutturare il *software* di analisi, quali dati inserire nel sistema, quali indagini far svolgere alla macchina, in *quali* (e in *quale* segmento temporale delle) procedure aziendali prevederne l'applicazione (sul punto, in particolare, si veda lo studio DGI (2017)12, pubblicato dal Consiglio d'Europa, dal titolo: *Algorithms and Human Rights. Study on the human rights dimensions of automated data processing techniques and possible regulatory implications*, p. 6). Si tratta di procedure polimorfe, in grado cioè di assumere rilievo, a seconda delle tecniche con cui sono costruite e implementate, sia nell'ambito del *risk assessment*, che nell'ambito del *risk management*.

Queste analisi informatiche dei dati, infatti, potranno essere soltanto strumenti di analisi e valutazione (e *non* anche di gestione) del rischio ove l'impresa decida di condurle sulla base di una logica *ex post*, sottoponendo cioè semplicemente a revisione il proprio patrimonio informativo (interno ed esterno) per identificare aree sensibili ed esposte al verificarsi di illeciti, senza rendere tali strumenti parte integrante dei singoli protocolli operativi di controllo del rischio reato. Invero, in tali casi l'anomalia documentale verrebbe rilevata in un momento in cui la procedura di formazione della volontà dell'impresa si è conclusa. In una fase, quindi, in cui l'eventuale corruzione si è già consumata – con il conseguente radicamento della responsabilità da reato della società.

Ciò non vuol dire che meccanismi così strutturati non abbiano alcuna utilità rispetto alla costruzione dei modelli organizzativi. Più semplicemente si tratterebbe di tecniche di miglioramento pro-futuro della compliance interna all'organizzazione complessa. Ove, infatti, la base di dati oggetto dell'indagine

venga costruita attraverso metodologie credibili – prevedendo l'obbligo di inserire nel sistema IT ogni informazione rilevante e costruendo effettive sanzioni disciplinari nei confronti dei dipendenti per le relative violazioni di tali obblighi di *Disclosure* interni – l'attività di *risk assessment* risulterebbe particolarmente valida ed efficace, identificandosi i fattori di rischio sulla base di una ricognizione completa di ogni dato di possibile rilievo e con le straordinarie capacità di calcolo e comparazione di un sistema informatico. Ciò, certamente, potrebbe rappresentare un elemento di rilievo di cui tener conto per valutare le opportune modifiche ai protocolli di gestione del rischio reato e consentirebbe di rafforzare notevolmente la tenuta complessiva del sistema di compliance, anche rispetto alla temutissima valutazione del giudice sull'idoneità del modello. Come visto, infatti, in tal caso le esigenze di gestione del rischio verrebbero rilevate da una pervasiva analisi condotta sulla base dell'intero patrimonio informativo rilevante dell'organizzazione complessa di riferimento e con metodologie di analisi di dati in grado di individuare profili di criticità a volte non identificabili altrimenti.

Tali meccanismi, peraltro, consentono di allocare efficacemente i costi della compliance verso i settori di attività dell'impresa che più necessitano di attenzione in tal senso, evitando lo spreco di risorse.

(B) Nondimeno, spingendoci oltre, va rilevato come le società potrebbero decidere di compiere un passo ulteriore, prevedendo l'applicazione di tali strumenti non soltanto nella direzione appena indicata, ma anche nei singoli protocolli operativi di gestione del rischio corruzione, facendo riferimento nel modello organizzativo all'utilizzo di questi meccanismi di *risk detecting* nelle proprie operazioni quotidiane.

Ciò, nella prassi, accade principalmente rispetto alle procedure di c.d. *due diligence* nei confronti di terze parti, ove ogni procedura decisionale in merito all'opportunità di intraprendere un determinato affare è anticipata dalle predette attività di data *analytics,* con la previsione di un report in *real time* al management in merito alle eventuali anomalie rilevate e ai conseguenti rischi legali e di non conformità connessi ai possibili rapporti da intraprendere con il singolo partner/agente commerciale (specie per affari all'estero rispetto ai quali può esistere un rischio di corruzione internazionale). In tali casi, l'attività di *big data Analytics* diventa un vero e proprio strumento concreto di prevenzione, innervato nei protocolli di controllo del rischio reato.

Una simile procedimentalizzazione delle attività, peraltro, se correttamente strutturata ponendo attenzione agli aspetti critici sopra segnalati in termini di affidabilità e completezza dei dati oggetto di analisi, potrebbe ritenersi un utile strumento per costruire un meccanismo di prevenzione tale da non poter essere eluso se non ricorrendo a condotte fraudolente e di notevole complessità tecnica. Così rafforzandosi notevolmente l'apparato di *compliance* della persona giuridica in relazione all'*enforcement* del d.lgs. n. 231 del 2001. Non mancano, tuttavia, le ombre nello scenario sin qui delineato.

Adottare il già menzionato strumento di *report in real time* al *management*, infatti, se da un lato rafforza l'idoneità preventiva (astratta) del *compliance program*, dall'altro si espone a facili censure di non efficace attuazione del modello (chiaramente allorquando il pericolo segnalato sia ignorato dagli organi aziendali). Un profilo, quest'ultimo, su cui come noto molto spesso si appuntano le decisioni che negano l'efficace esimente del modello nei procedimenti per responsabilità da reato delle persone giuridiche. Ancora, in termini più generali si è rilevato come l'automazione della *compliance* potrebbe dar luogo a una modifica della base fattuale su cui oggi si basa la responsabilità da reato delle imprese, ponendo non indifferenti problemi rispetto alla possibilità di ritenere sussistente la colpa in organizzazione della persona giuridica – specie allorquando la commissione dell'illecito penale sia stata resa possibile da un difetto di progettazione del sistema informatico di prevenzione che l'impresa si limita a utilizzare, senza esserne l'autore.

L'effettiva messa in atto di alcune di queste pratiche di sorveglianza generalizzata apre poi l'ulteriore profilo dell'eventuale ammissibilità di simile procedure rispetto alla disciplina dei controlli sui lavoratori, nonché in tema di tutela della *privacy* e del c.d. domicilio informatico del dipendente: basti pensare, a quest'ultimo riguardo, al consolidato orientamento della giurisprudenza della Corte di Cassazione in termini di configurabilità del reato di accesso abusivo a sistema informatico nel caso di controllo delle e-mail dei dipendenti (pubblici o privati).

L'implementazione di queste procedure, peraltro, può sollevare a volte il tema della legittimità del trattamento dei dati personali dei soggetti coinvolti dalle indagini informatiche, anche in considerazione del fatto che l'art. 22 del Regolamento europeo sulla protezione dei dati personali vietano le decisioni basate unicamente su trattamenti automatizzati e stabiliscono il diritto dell'interessato di ottenere l'intervento umano nel procedimento di formazione di volontà da parte del titolare del trattamento. Una problematica, quest'ultima, che potrebbe a ben vedere verificarsi anche con riferimento all'utilizzo dei già menzionati sistemi di *data analytics* nell'ambito delle attività di *compliance*.

Infatti, l'*output* prodotto dai s*oftware* in parola non soltanto potrebbe basarsi su un trattamento di dati integralmente automatizzato e senza alcun intervento umano di "mediazione valutativa" del risultato dell'analisi, ma potrebbe determinare la scoperta di elementi fattuali indizianti a carico di (o l'assunzione di decisioni disciplinari o di altra natura in vario modo impattanti su) diversi dipendenti o altri soggetti coinvolti nell'analisi informatica. Peraltro, la possibilità concreta che attraverso l'uso della big data *analytics* possano individuarsi elementi indizianti a carico di persone fisiche solleva l'ulteriore problematica delle connessioni che possono istaurarsi tra queste procedure di compliance e le *corporate internal investigation*, anche perché le pratiche in analisi potrebbero esse stesse diventare uno degli strumenti attraverso cui l'impresa può svolgere le proprie indagini interne. E ciò, chiaramente, impone di individuare il sistema di garanzie da riconoscere ai soggetti coinvolti.

Senza contare, poi, come si anticipava, le difficoltà connesse alle (limitate) possibilità di contestare il risultato cui il sistema informatizzato sia pervenuto in considerazione della complessità di comprendere le modalità (spesso oscure) attraverso cui la macchina ha optato per una determinata soluzione valutativa.

Insomma, a fronte degli indubbi vantaggi che, come visto, l'implementazione di questi sistemi potrebbe determinare nel rafforzare il sistema di *compliance* anticorruzione delle persone giuridiche, l'utilizzo di tali *software* espone oggi l'impresa a rischi legali su versanti diversi, ma non meno delicati, e per la cui gestione è indispensabile un approccio multidisciplinare.

Là dove, quindi, lo svolgimento di simili attività di *compliance* dovesse trovare in futuro sempre maggiore riscontro nella prassi, non potrà che essere il legislatore a farsi carico di regolare la materia, bilanciando correttamente i diversi interessi in gioco. Non si può, del resto, "scaricare" sul privato un compito tipicamente pubblicistico come quello di prevenire reati e fenomeni illeciti senza fornire a tali soggetti adeguati strumenti (anche normativi) per svolgere tale ruolo e anzi sanzionando le imprese che si avvalgono di innovative metodologie di gestione del rischio.

3. Considerazioni conclusive

Lo sforzo che si è sin qui compiuto è stato quello di illustrare il funzionamento degli strumenti di *data analytics* nel settore della *compliance* (anzitutto anticorruzione) nei settori pubblico e privato e di mettere in risalto alcuni punti di frizione con diritti fondamentali del singolo.

Si tratta di un orizzonte che, a prima vista, sembra ancora lontano, riservato a strutture organizzative complesse all'avanguardia, e destinato solo in futuro ad assumere contorni più precisi.

La rapida evoluzione della tecnologia e la sua costante diffusione ci dicono tuttavia che, prendendo a prestito le oramai celebri considerazioni del Presidente della Corte Suprema degli Stati Uniti Roberts, il futuro è già tra di noi. L'insegnamento che proviene, come visto, dall'utilizzo degli algoritmi predittivi, in chiave di prevenzione della criminalità e in fase di decisione giudiziale sul quantum di pena, è davvero eloquente.

Quell'esperienza deve essere da monito anche per gli altri settori in cui oggi si affaccia il tema dell'impiego dell'AI per individuare fonti di rischio-reato e progettare idonee misure preventive.
Se, come appare verosimile, si diffonderanno i sistemi di analisi di quantità enormi di dati, si porrà l'esigenza di approntare, sulla scia magari di una regolamentazione del fenomeno nell'ambito pubblico, una disciplina anche nel settore privato.

Quali dunque le linee portanti di siffatta disciplina?

(A) Ci sembra che possa essere di aiuto il dibattito maturato rispetto alla possibile riforma del D.lgs. n. 231 del 2001 circa la necessità di procedere a una positivizzazione dall'alto delle cautele di cui richiedere l'adozione agli enti collettivi.
In questa prospettiva potrebbe infatti trovare spazio anche una presa di posizione legislativa in merito all'individuazione di uno standard minimo delle tecniche di costruzione e utilizzo di questi sistemi.
Infatti, uno degli aspetti più delicati emerso dalla dinamica applicativa del D.lgs. n. 231 del 2001 è legato, come noto, alla pressoché totale assenza di decisioni che riconoscano l'idoneità preventiva dei modelli organizzativi, tenuto conto del fatto che il legislatore non fornisce alle imprese nient'altro che indicazioni di massima sull'ossatura del compliance program.
Da qui la proposta, appena richiamata, di positivizzare per settori differenziati le cautele da imporre all'impresa, stabilendo una presunzione di idoneità relativa del modello organizzativo conforme alle indicazioni legislative.
Nella materia anticorruzione, quindi, l'implementazione di queste procedure di *big data analytics* potrebbe costituire una delle indicazioni da fornire all'impresa in merito alle cautele da implementare per costruire il proprio sistema di compliance.
Ciò, ovviamente, a patto che il legislatore chiarisca esattamente e nel modo più preciso possibile le fonti di dati da analizzare, le indagini da far compiere al sistema e le metodologie di analisi.

(B) Una soluzione equilibrata potrebbe peraltro essere quella di prevedere un'ulteriore cautela per l'impresa consistente nella registrazione di ogni transazione aziendale di rilievo, istituendo un apposito sistema di controllo interno per verificare che ogni operazione di disposizione di *asset* aziendali si svolga nel rispetto delle *policy* di prevenzione del *management* dell'impresa, e ciò anche al fine di rafforzare la completezza e l'affidabilità della base di dati da sottoporre a indagine informatica.
Si tratterebbe, del resto, di una scelta di regolazione non sconosciuta ad altri ordinamenti, seppur nella differente ottica dell'istituzione di un vero e proprio obbligo legale: negli Stati Uniti, per esempio, le *Accounting Provisions* del *Foreign Corrupt Practices Act* prevedono per l'appunto obblighi di registrazione di tal fatta e l'implementazione di un connesso sistema di controllo interno a carico di alcune società emittenti strumenti finanziari negli USA.

(C) Un altro tema, infine, potrebbe essere quello di sfruttare il patrimonio informativo prodotto dai *software* di analisi per procedure di *self reporting* alle autorità pubbliche. Procedure cui eventualmente collegare benefici di intensità graduabile: dalla riduzione del carico sanzionatorio alla radicale non punibilità per l'impresa che si autodenuncia.

Il legislatore, infatti, potrebbe ritenere che il rischio evidenziato, in relazione a tali procedure, di una strumentalizzazione dell'autodenuncia possa essere superato affidando interamente al sistema informatico il compito di individuare gli elementi alla base della *Disclosure*, eliminando il filtro dell'uomo e costruendo il *software* in modo tale che non possa essere artificiosamente modificato.
Non ci nascondiamo peraltro come quest'ultima prospettiva non sia di facile realizzazione e rischi di creare molti più problemi di quanti in realtà ne possa risolvere.

Quel che è certo, tuttavia, è che in un modo o nell'altro il tema della premialità per le imprese virtuose, che impiegano con spirito proattivo ingenti risorse nelle loro attività di *compliance*, dovrà essere affrontato. Il sistema, insomma, prima o poi dovrà fare i conti con sé stesso, offrendo alle imprese un quadro di regolazione moderno per implementare le attività di prevenzione del rischio reato, ma stabilendo al contempo meccanismi e regole di comportamento chiari, osservati i quali l'impresa possa nutrire la ragionevole aspettativa di andare esente da responsabilità.

29 marzo 2021